IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 2, 2018, accepted September 1, 2018, date of publication September 24, 2018, date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2871762

A Comprehensive Overview of Government Hacking Worldwide

CHEN-YU LI[1], (Student Member, IEEE), CHIEN-CHENG HUANG[2], FEIPEI LAI[3], (Senior Member, IEEE), SAN-LIANG LEE[4], (Senior Member, IEEE), AND JINGSHOWN WU[1], (Life Fellow, IEEE)

[1]Graduate Institute of Communication Engineering and Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan
[2]Department of Information Management, National Taiwan University, Taipei 10617, Taiwan
[3]Computer Science and Information Engineering and Electrical Engineering Departments, National Taiwan University, Taipei 10617, Taiwan
[4]Department of Electronic Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan

Corresponding author: Chen-Yu Li (d00942021@ntu.edu.tw)

ABSTRACT There has been an ongoing and heated public policy debate on the appropriate role of and limitations to government hacking in maintaining a proper balance of national security and privacy. Asserting that they are compelled to use government hacking tools to protect their countries and populations, law enforcement and government agencies are increasingly strident in expressing the importance of accessing and intercepting encrypted communication data. However, many non-governmental and civil society organizations and activists strongly oppose government hacking because they consider its methods and techniques are extremely invasive and potentially compromising to the fundamental right of privacy. They are also concerned that the implementation of hacking techniques or similar methods would weaken encryption standards and place the security of the Internet at risk. This paper presents an overview of the current status of government hacking and discusses challenges to lawful interception (LI) technology and rules. The current state of LI and government hacking in five countries is reviewed, and capability is assessed in terms of several widely publicized events, in an effort to analyze the limitations of current solutions. Finally, the open challenges to and future direction of government hacking are highlighted.

INDEX TERMS Communication system and network security, government hacking, law enforcement, lawful interception, social network services, surveillance, national security, privacy.

I. INTRODUCTION

From the inception of the telecommunications industry in the 19th century up to relatively recently, telephony constituted the primary mode of communication [1]. The basic principle of voice-based telecommunication relies on the use of circuit-switching networks, in which initiating a phone call results in the setup of a continuous circuit [2] in which one or more switches are connected by trunks along a path over the duration of the call. When one of the parties hangs up, the switches are disconnected and the released resource is available to other call requests [2]. The earliest interceptions were implemented by tapping additional wires at points between the central office of the telecommunication service provider and the subscriber [3]. These additional wires carried the intercepted signal to a pair of earphones and/or a recorder manned by law enforcement officers. The officers could thereby listen in on the voice communications of a suspect. Starting in the 1990s, mobile digital voice telecommunication services surged in popularity, resulting in a substantial transformation of the telecommunication industry. This made it more difficult for law enforcement agencies to execute lawful interception (LI) procedures. In response, many countries enacted new LI rules [4]–[6], with one example being the Communications Assistance for Law Enforcement Act (CALEA) in the United States [7]. Such acts, however, typically require the cooperation of ''telecommunications carriers'' to embed a lawfully authorized government interception function into their network [8]. There is therefore a watershed in the literature on government surveillance, with most studies prior to the growth of the Internet focusing on how to intercept general telecommunications [9], while later studies focus on voice over IP (VoIP) and other Internet-based communication technologies [9]–[13]. With the coming of the Internet era, new LI standards for VoIP and other Internet-based telecommunication services have been established by several international standard organizations [12], [14]–[21].

This expansion of coverage has been extremely helpful to law enforcement agencies [22]–[24]. However, as communication service providers continue to offer increasingly sophisticated services and the number of novel communication services not covered by conventional telecommunication service providers multiplies [25], [26], the regulatory gap continues to widen, and modern services such as webmail, social networks, and peer-to-peer communications are still not covered by conventional interception regulation [27], [28].

The increasing variety of powerful smart devices has also changed user behavior and the functionality of popular Internet-based communication services. The relationship between subscriber and service provider has changed from one between a user and a single telecommunication service provider, to one in which the user multiply accesses many Internet-based communication providers [29]–[34].

Such communication services are generally protected by proprietary encryption mechanisms [35]–[37] that are no longer standardized. Many providers also operate globally [38] and not necessarily in compliance with local interception rules. Furthermore, the ways in which communications services are obtained is also becoming more varied and complex [39], [40].

As a result of these pronounced market changes, enforcement agencies can still obtain court orders to execute authorized interception of communications from suspects, but service providers often lack the technical ability to carry out these orders. When service providers are able to cooperate with law enforcement in developing and deploying interception mechanisms, such orders are sometimes simply not fully carried out. To further complicate matters, developing and deploying an appropriate interception mechanism can take months or years, during which time potentially critical information can be lost. This situation is often called the ''going dark'' problem [27].

Currently, there is no solution directly equivalent to traditional interception standards that are widely available to law enforcement agencies around the world for solving the ''going dark'' problem. One proposed—but very controversial—solution is government hacking [41]–[44].

Using hacking techniques for surveillance is not a new approach, with the literature revealing that law enforcement agencies have been using such tools to aid in investigation since at least 1998 [40], [45]. Prior to the development of hand-held smart devices, internet-based communication services were available only on home or office computers on which surveillance tools could be installed by law enforcement with relative ease. By contrast, it is now possible to communicate through encrypted channels at any time or place via various services and smart devices, which has made surveillance of suspects' communication more challenging.

Many studies have assessed the privacy impacts introduced by government hacking [7], [39], [46]–[53]. Further, there has been limited focus on the current status, techniques, and challenges of government hacking. This paper summarizes the status of government hacking under the regulatory frameworks of various countries and through the lens of several hacking events. The results are then further analyzed to assess potential balancing solutions to address the tensions arising from the collision of law enforcement, technology, privacy, policy, public safety, and information security. Starting with an overview of current LI regulations, the standards, challenges, and necessity of using government hacking are discussed. Along with government hacking regulations in the countries of focus in this report, the application of hacking techniques in the field are described and, finally, future challenges and developments are described. Although many media outlets and organizations have published news regarding LI and government hacking activities from a lot of different countries, the basic principles, frameworks, and techniques of LI and government hacking are often similar. Therefore, we mainly focus on the states of these five countries in this work.

II. CURRENT LAWFUL INTERCEPTION CHALLENGES

LI, which is also known as lawfully authorized electronic surveillance [54], is a legal procedure in which network operators or communication service providers allow law enforcement or intelligence agencies to surveil the communications of individuals or organizations. This can be crucial to investigating serious criminal activities, stopping terrorism, or protecting national security. In this section, we introduce the current state of LI by focusing on standards, regulations, and confronted challenges.

A. LAWFUL INTERCEPTION STANDARDS AND THEIR PROCESS

Many countries use LI standards to provide economically and technically feasible surveillance solutions that are in accordance with national and international conventions and legislation. Standards for use in various types of networks and services have been established by a number of standards organizations, including the 3rd Generation Partnership Project (3GPP) [55]–[57], the Alliance for Telecommunications Industry Solutions/ Telecommunications Industry Association (ATIS/TIA) [20], [54], CableLabs [19], the European Telecommunications Standards Institute (ETSI) [58], [59], and the Internet Engineering Task Force (IETF) [60] (Table 1).

In general, LI relies on three fundamental functionalities: access, delivery, and collection [61]. The access function (AF) typically involves one or more intercept access points (IAPs) [20] or internal interception functions (IIFs) [62]–[64], in which intercepted communications and related information on a suspect are separated. This function can vary by network and service provider [20]. The delivery function (DF) is used to deliver intercepted communications to the collection function (CF) [20]. The internal network interface (INI), which is placed within the internal network of the provider, is used to connect between the AF and DF [61].

There are two distinct types of DF channels. The first are ''call content channels'' (CCCs) [20], also known as

TABLE 1. Summary of major LI standards.

Organization	Standard No.	Current Version (Published Date)	Standard Title
3GPP	TS 33.106	V14.1.0 (2017-06)	3G security; Lawful interception requirements
	TS 33.107	V14.2.0 (2017-09)	3G security; Lawful interception architecture and functions
	TS 33.108	V14.2.0 (2017-09)	3G security; Handover interface for lawful interception
ATIS/TIA	J-STD-025	J-STD-025-A (2003-04)	Lawfully Authorized Electronic Surveillance
	J-STD-025	J-STD-025-B (2013-03)	Lawfully Authorized Electronic Surveillance
ATIS	1000678	ATIS-1000678.b.v2.2010 (2015-07)	Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks
CableLabs	PacketCable 2.0	PKT-SP-ES-DCI -C01 (2014-03)	Delivery Function to Collection Function Interface Specification
	PacketCable 2.0	PKT-SP-ES-INF -C01 (2014-03)	Intra-Network Functions Specification
ETSI	TS 101 671	V3.14.1 (2016-03)	Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
	ES 201 671	V3.1.1 (2007-05)	Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
	ES 201 158	V1.2.1 (2002-04)	Telecommunications security; Lawful Interception (LI); Requirements for Network Functions
	TS 101 331	V1.5.1 (2017-03)	Lawful Interception (LI); Requirements of Law Enforcement Agencies
	TS 102 232-1 ~TS 102 232-7	Individual	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery Series
	TR 102 503	V1.11.1 (2017-11)	Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and Retained data handling Specifications
	TR 102 519	V1.2.1 (2014-02)	Lawful Interception (LI); Lawful Interception of public Wireless LAN Internet Access
	TR 102 528	V1.1.1 (2006-10)	Lawful Interception (LI); Interception domain Architecture for IP networks
	TR 102 519	V1.2.1 (2014-02)	Lawful Interception (LI); Lawful Interception of public Wireless LAN Internet Access
	TS 101 909-20-1	V1.1.2 (2005-10)	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 1: CMS based Voice Telephony Services
	TS 101 909-20-2	V1.2.1 (2006-03)	Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub-part 2: Streamed multimedia services
IETF	RFC 3924	2004 (2004)	Cisco Architecture for Lawful Intercept in IP Networks

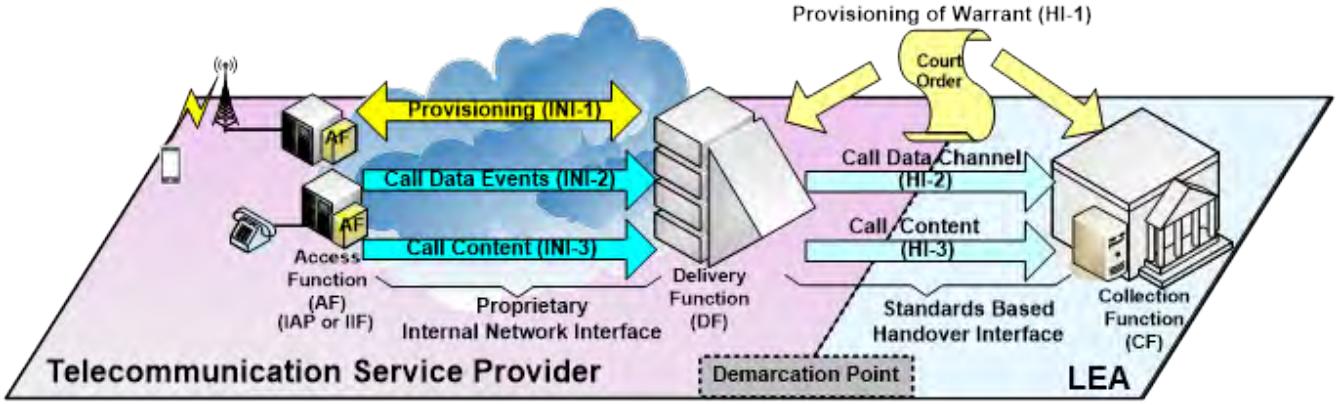

FIGURE 1. Generic view of LI architecture [61].

"handover interface port 3" (HI3) channels [54], [62], which are used to forward call content such as voice or data communications. The second are known as "call data channels" (CDCs) [20] or "handover Interface port 2" (HI2) channels [54], [62] and are used to forward messages containing call-identifying information such as the caller and callee identities. The CF or "Law Enforcement Monitoring Facility" (LEMF) is maintained by the law enforcement agency (LEA) and used to gather and analyze intercepted voice/data and identifying information [54], [61]. The collection facility coordinates delivered messages to maintain the association between current state information and call content [20], [65]. Figure 1 shows a generic view of the LI standard architecture [61].

The general process flow of LI can be described as follows: when the authorization authority, such as a court of law, issues

TABLE 2. Summary of lawful interception obligations for providers in five countries.

Country	Australia	France	Germany	The United Kingdom	The United States
Title of the act or regulation	Telecommunications Act 1997 and Telecommunications (Interception and Access) Act 1979	The French Postal and Electronic Communications Code (Code des postes et des communications électroniques, CPCE)	The German Telecommunication Act (Telekommunikations gesetz, TKG)	The Regulation of Investigatory Powers Act 2000 (RIPA)	Communications Assistance for Law Enforcement Act (CALEA)
Which type of provider is regulated under the law	The carriers and carriage service providers [66], [67]	Operators [70], [72]	A person operating a system through which publicly available telecommunications services are provided [75], [76]	Public telecommunications services providers [79]	Telecommunications carriers [85], [86]

a court order for LI to the LEA, the LEA passes this order to the telecommunication provider. The provider determines the relevant target identities from the information given in the order and then causes its AF to be applied to these target identities. After the telecommunication provider finishes this work, it informs the LEA that the court order has been received and acted upon. At the same time, the information related to the target identities needs to be passed on, along with identification that is used for correlating the target and their call content and call data. The call content and call data of this target are delivered from the AF to DF of the telecommunication provider. The DF forwards these data to the CF of the LEA.

B. THE LAWFUL INTERCEPTION OBLIGATION OF PROVIDERS

LI has already become a basic obligation and requirement of telecommunication networks and services providers in nearly every country, with access, network, and service providers required to maintain the interception capabilities needed to access all applicable communications by specified targets without gaps in coverage. In the following, we discuss the interception obligations of providers in Australia, France, Germany, the United Kingdom, and the United States; these are also summarized in Table 2.

1) AUSTRALIA

One obligation under the Telecommunications Act 1997 and the Telecommunications (Interception and Access) Act 1979 (the TIA Act) [66] is for networks, carrier facilities, and carriage service providers (CSPs) to be able to intercept all communications passing through their systems [66], [67]. In this context, carriers are defined as the entities who handle telecommunications network units that provide telephone, internet access, VoIP, and other carriage services to the public [68], [69], while CSPs are defined as entities that use telecommunications network units to supply carriage services to the public.

All carriers and some CSPs are also required to submit an annual interception capability plan outlining their interception policies and strategies on how to comply with their obligations [68], [69] to a communications access coordinator, who serves as the primary point of contact between interception agencies and telecommunications carriage service providers.

2) FRANCE

Under Article D98-7-III of the French Postal and Electronic Communications Code (Code des postes et des communications électroniques, or CPCE) electronic communications network operators in France have an obligation to implement the measures necessary to allow the implementation of interception capabilities. Only qualified agents are authorized to use and control interception systems [70], [71].

According to Article L32 of the CPCE, electronic communication is defined as the "broadcast, transmission or reception of signs, signals, writings, images, or sounds by electromagnetic means" [72], [73]. Under Article 100 of the Criminal Procedure Code (Code de procédure pénale, or CPP), the interception of correspondence sent by electronic communications is referred to as "the interception, registration and transcription of correspondence sent via electronic communications" [73], [74], which means that it includes the interception of correspondence sent or received on different platforms including landlines, mobile phones, tablets, and computers [73]. Under Article 706-102-1 of the CPP, the interception of communication is authorized for forms of communication including telephone and mobile phone services, VoIP calls, emails, and instant messaging [71].

3) GERMANY

Under Section 110 of the Germany Telecommunication Act (Telekommunikationsgesetz, TKG), any entity operating a telecommunications system through which publicly available telecommunications services are provided

TABLE 3. Origin of major Going Dark issues impacting lawful interception.

Issues	Encryption communications and data	Different devices, operating system and applications	International and individual providers	Nomadic Internet access
Causes	1. Use of low-cost encryption 2. Large numbers of applications on the market 3. Embedding of encrypted mechanisms in most applications 4. Conventional LI facilities find it difficult to access plaintexts of third-party communication services 5. Difficult to break down encrypted mechanisms	1. Numerous brands and types of devices 2. Variable operating systems and architectures 3. Exponential growth in applications 4. Law enforcement agencies lack research and budget for interception	1. Provide services via the Internet 2. Store data in worldwide hosts 3. Do not necessarily follow local law enforcement rules 4. Do not necessarily follow local interception rules 5. Do not necessarily provide metadata for services	1. Operate via numerous anonymous or free Internet access points 2. Separate access of individual services and providers 3. Difficult to find the real geo-location of a user

should provide technical facilities for implementing telecommunications-provided interception measures [75], [76], i.e., public telecommunication service providers in Germany are required to maintain technical capabilities and facilities to execute interception. More detailed interception requirements and technical specifications are given in the Telecommunications Interception Ordinance (Telekommunikations-Überwachungsverordnung, or TKÜV) [75] and in the corresponding technical guideline for the implementation of the measures for the surveillance of telecommunications and the disclosure of information (Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation und zum Auskunftsersuchen für Verkehrsdaten, or TR TKÜV) [77], [78]. In this context, communications that can be intercepted include conventional telephone and mobile phone services, VoIP calls, and emails [78].

4) THE UNITED KINGDOM

Section 12 (Maintenance of Interception Capability) of the Regulation of Investigatory Powers Act 2000 (RIPA) [79] and the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 [80] contain provisions regarding the interception of communications transmitted by means of a public telecommunications service. According to Section 2 of RIPA, a ''telecommunication service'' is defined as any service that provides access to, or facilities for making use of, any telecommunication system [81]. This Section is clearly intended to cover any service that facilitates the creation, management, or storage of communications that are or may potentially be transmitted, which under this definition includes not only conventional telephone and mobile phone services but also Internet-based services, such as VoIP, web email, instant messaging applications, and cloud-based services [82], [83].

5) THE UNITED STATES

The Communications Assistance for Law Enforcement Act (CALEA) affirms the duty of telecommunication carriers to cooperate in the interception of communications for ''law enforcement purposes, and other purposes'' [84]. Section 103 (Assistance Capability Requirements) of CALEA requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have interception capabilities [85]. Here, a telecommunications carrier is defined as ''a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire,'' but does not include information service providers involved in ''generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications'' [86].

All communications services or facilities that utilize circuit or packet mode equipment, facilities-based broadband Internet access providers, and interconnected VoIP services are subject to CALEA [87].

C. MAJOR ISSUES REGARDING THE IMPACT OF ''GOING DARK'' ON LAWFUL INTERCEPTION

In the previous section, we saw that LI regulations and standards primary cover conventional telecommunication services, with some covering information services as well. Even when law enforcement agencies are granted the legal authority to intercept some partial communications and information pursuant to a court order or warrant, in many cases they will not have the technical capacity to intercept and access a suspect's data [88]–[90]. The ''going dark'' problem has become the most serious challenge to global law enforcement [27], [73], [90], and conventional interception techniques face difficulties in addressing currently popular internet-based over-the-top (OTT) communication modalities. The characteristics of modern communications techniques that enhance the ''going dark'' problem are discussed below and listed in Table 3.

1) ENCRYPTION COMMUNICATIONS AND DATA

For data security purposes, mechanisms such as end-to-end encryption have been embedded in many popular

TABLE 4. Comparison of potential solutions for Going Dark.

Potential solutions	Require providers to offer decrypted keys	Require that providers encrypt communications and information	Require providers to build functionality	Block encrypted services	Use Government Hacking
Solution provider	Individual service provider	Individual service provider	Individual service provider	All internet service providers (ISP)	Developed by governments or third-party providers
Technical complexity	Low (Only necessary to obtain decryption keys from individual service providers)	Low (Obtain plaintext data from service providers)	Medium (Requires each service provider to develop interception mechanisms)	Medium (Deploys deep packet inspection (DPI) or similar network equipment in all Internet service providers within a country)	High (Develops individual tools for each service without the service provider aid)
Implementation ability	Very Difficult (Service providers reluctant to provide keys for commercial reasons; international companies or individuals not subject to local laws)	Very Difficult (Service providers reluctant to provide keys for commercial reasons; international companies or individuals not subject to local laws)	Very Difficult (Service providers reluctant to provide keys for commercial reasons; international companies or individuals not subject to local laws)	Difficult (Possible to block well-known services but difficult to block newest services in a timely manner)	Difficult (Necessary to identify all types of known exploits and zero-days or to use social engineering/physical contact methods to infect suspect's equipment/access their data)
Implementation cost	Low (Requires only decryption keys)	Low (Requires plaintext data from providers)	High (Need to develop the interception system for each service)	Very High (Deploy extensive equipment in all ISP networks in country)	Very High (Develop individual tools for each service)
Factor dominating the implementation cost	Service providers themselves design the decrypted program	Service providers themselves design the decrypted program	Decrypted programs designed by service providers themselves; each LEA must build intercept system for each service	Deploy network equipment (dependent on the number and capacity of links in each ISP)	Find possible exploits or zero-days for each service or device

communication applications [34], [36], [91], social media platforms [92], and mail services [93], [94]. Because so many devices now use encryption mechanisms [95], law enforcement agencies are finding it difficult to obtain valuable intelligence from them for investigation purposes.

2) DIFFERENT DEVICES, OPERATING SYSTEM AND APPLICATIONS

Worldwide smartphone shipments are expected to rise from 1.47 billion in 2016 to over 1.70 billion in 2021 [96]. The main providers of smartphones include Samsung, Apple, Huawei, OPPO, vivo, Xiaomi, LG, etc. [97], [98]. Google's Android operating system (OS) occupies nearly 85% of the worldwide smartphone market, with Apple's iOS and other prominent OSs such as Blackberry and Windows mobile comprising 14–15% of the market [96]. Recently introduced OSs that can be custom-installed on a smartphone include Tizen, Plasma Mobile, PureOS, postmarketOS, LineageOS, eelo, and Sailfish OS [99].

At the same time, the number of mobile applications has also grown rapidly. Apple's App Store, which was launched in 2008 with 500 apps, grew to 2.2 million apps in 2017 [33]. The Google Play Store, which has followed a growth path similar that of the App Store, now provides 2.8 million applications [33]. Law enforcement simply does not have the resources to research and develop investigatory tools to cover the huge number of devices, OSs, and applications.

3) INTERNATIONAL AND INDIVIDUAL PROVIDERS

Devices, operating systems, and applications are provided over a global market comprising many companies and individuals who cannot realistically be required under each court order to aid every government agency in intercepting communications or accessing information and metadata.

4) NOMADIC INTERNET ACCESS

The Internet can be accessed via mobile data connections or Wi-Fi hotspots. This allows users to change their connection configuration at will, a nomadic property that can render law enforcement incapable of finding or identifying suspects or crime scenes.

D. POTENTIAL SOLUTIONS FOR "GOING DARK"

Several potential solutions for the "going dark" issue are listed in Table 4 and discussed below.

1) REQUIRE PROVIDERS TO OFFER ENCRYPTION KEYS

This solution is also called "key escrow [100]" or "Government access to keys" (GAKs) [101], [102]. The basic

idea behind GAK is to provide safe cryptosystems for secure communication without preventing law enforcement from doing its job [101]. Under a court order for interception, an LEA would be able to intercept encrypted data and decipher messages by obtaining specific key components from two separate key escrow agencies [100], [101].

2) REQUIRE THAT PROVIDERS DECRYPT COMMUNICATIONS AND INFORMATION

Under this scheme, providers avoid releasing their cipher/decipher keys by instead providing law enforcement agencies that need to access communications or data with deciphered plaintext [103].

3) REQUIRE PROVIDERS TO BUILD INTERCEPTION FUNCTIONS

Under LI standards, telecommunication service providers can themselves embed interception functions into their services or applications [104], [105].

4) BLOCK ENCRYPTED SERVICES

Under this solution, a government can require Internet access service providers to block third-party encrypted communication services [104], forcing suspects to use communication methods, such as 2G/3G voice call or voice over long-term evolution (VoLTE) that can be intercepted.

5) GOVERNMENT HACKING

Generally speaking, government hacking involves the use of government-developed or purchased malware to intercept a suspect's communications or access their information. In this context, malware refers to a program used to break the operation of or obtain operating authority over a computer system [106].

In Table 4, we compared these different solutions. It is seen that government hacking is an expensive, complicated, and even risky solution. However, it is currently the most widely used solution worldwide because nearly all other potential solutions require obtaining support from service providers. Cases in which a provider supports the LEA in conducting an investigation can in fact be carried out in a manner similar to conventional LI operations or legal frameworks, allowing the investigation to proceed smoothly. In practice, many service providers do not fully accept LEA requirements [88], [107], [108] and some crucial information is unobtainable. Some researchers have even suggested that having a service provider build decryption tools or embed LI functionality is an essentially insecure process [53].

Of course, an LEA can also try to block a suspect's communications to compel them to use communication channels with embedded LI functionality. Under such a solution, the LEA builds a ''block wall'' for traffic filtering purpose over an ISP's backbone networks, which requires significant government expenditure. Furthermore, the nomadic Internet access feature means that a suspect can switch to different access networks or services to easily bypass the LEA trick, to block encrypted services. In some cases, savvy suspects can detect monitoring from subtle changes in their Internet user experience. As a result, many possible solutions can very easily fail and, ultimately, government hacking becomes the fallback solution to LEA investigatory challenges.

III. STATUS OF GOVERNMENT HACKING REGULATIONS WORLWIDE

In the previous section, we compared several potential solutions to the ''going dark'' challenges faced by many LEAs worldwide. It was determined that owing to its high technical complexity and cost and difficulty to implement, government hacking is not necessarily the best overall solution. However, under the many situations in which law enforcement has problems in obtaining cooperation from service providers [107], [108], government hacking has become a prominent intercept implementation solution [39], [109]. In this section, we provide an overview of the regulatory status of government hacking worldwide.

A. AUSTRALIA

Australia has no clear regulation giving law enforcement the authority to engage in government hacking. Nevertheless, several relevant Acts appear to imply some form of authorization.

1) AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION ACT 1979 (ASIO ACT)

This Act, which is apparently the major regulation covering government hacking by the Australian Security Service, endows the Australian Security Intelligence Organization with special powers, including interception and examination of mail, installation, and monitoring of surveillance devices, monitoring telecommunications, and remotely accessing computers [110]. It also authorizes the addition, copying, deletion, or modification of other data in computers or telecommunications facilities [111].

2) CRIMES ACT 1914

This Act has a provision under which an executing officer (acting on behalf of an LEA) can access data from a computer or data storage device (including data held at a remote location) [112]. This Act has been construed to allow for measures that can overcome the use of passwords, encryption technologies, and cloud storage services [113].

3) THE SURVEILLANCE DEVICES ACT 2004 (SDA)

This Act provides the procedures under which officers of LEAs in Australia can obtain warrants, emergency authorizations, and tracking device authorizations for the installation and use of surveillance devices [114]. Under the Act, the definition of a data surveillance device is ''any device or program capable of being used to record or monitor the input of information into or the output of information from, a computer,'' where a ''computer'' is in turn defined as ''any electronic device for storing or processing

information [114]." A surveillance device warrant authorizes the use of a surveillance device on specified premises, objects, conversations, activities, or locations [114] and also allows for the installation, use, maintenance, and retrieval of equipment to enhance surveillance device performance, including devices to connect to the system used to transmit the information [114]. These stipulations imply permission to monitor digital devices such as desktop computers, laptops, smartphones, tablets, and other electronic equipment.

4) THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 (TIA)

In a previous section, we introduced the TIA Act as the major enabling regulation for law enforcement and security agencies to intercept telecommunications content and data in Australia [115]. Amendments inserted into the Act in 2006 enable "equipment-based interception" to intercept communications made via particular telecommunication devices that a person is using or is likely to use [116]. This language seems to imply that law enforcement requirements can be used to authorize government hacking techniques for accessing communications.

5) LAW ENFORCEMENT (POWERS AND RESPONSIBILITIES) ACT 2002:

This Act, proposed by the New South Wales (NSW) Government, has a provision under which LEAs are authorized to extend hacking techniques used on a given electronic system to facilitate the hacking of other electronic systems [117]–[119].

B. FRANCE

The French Code of Criminal Procedure (Code de procédure pénale) has legal provisions governing the use of hacking techniques, specifically, the amendments of LOI n° 2011-267 [120] and 2016-731 [121]. These provide for the legal use of information obtained "from the capture of computer data (De la captation des données informatiques)." Articles 706-102-1 to 706-102-9 in the French Code of Criminal Procedure appear to authorize the use of hacking techniques and tools by law enforcement for the purpose of gaining access to communications [122].

C. GERMANY

In 2008, the German Constitutional Court recognized that the government is allowed to access personal data and communications covertly under narrow conditions in which personal and public "life, limb, and freedom" are endangered [123], [124]. There are currently two main legal provisions for the use of hacking techniques in Germany: the Code of Criminal Procedure (StPO) [125], [126]; and the Federal Criminal Police Office Act (BKAG).

1) THE CODE OF CRIMINAL PROCEDURE

The monitoring and recording of telecommunications may, if necessary, be carried out through technical intervention in information technology systems used by a data subject to enable monitoring and recording (especially in unencrypted form), and communication content stored on a system may also be monitored and recorded if the data are encrypted during ongoing transmission through a public telecommunications network [125], [126]. The LEA must encrypt and hide their hacking tools, and no one aside from the investigators is authorized to read the data. The LEA can only monitor and record current communications or content passing through a public telecommunications network and can only effect necessary and reversible system changes for the purpose of data collection [125].

LEAs can use another technique called "Online-Durchsuchung" ("online searching") in which a suspect's device is intervened with for the purposes of collecting data that is not included in ongoing communication [125].

2) THE FEDERAL CRIMINAL POLICE OFFICE ACT (BKAG)

Under section 20k of the German Federal Criminal Police Office Act (BKAG), the officers are granted the power to use technical means to covertly intervene in information technology systems [127], [128]. This code authorizes BKAs to access information technology systems and permits covert remote searches of such systems. BKAs can collect data saved or stored on private or other computers used by a suspect (or data accessed from the cloud) to track their online behavior [129].

D. THE UNITED KINGDOM

Government hacking in UK is called "equipment interference" [130] and is used by LEAs and intelligence agencies to interfere with electronic equipment such as computers and smartphones with the goal of obtaining communications or equipment data or other information [130], [131]. There are two main legal provisions covering equipment interference.

1) INTELLIGENCE SERVICES ACT 1994

Equipment interference is authorized under Section 5 of the Intelligence Services Act (ISA) under a Code of Practice in which intelligence services are allowed to apply interference (whether remotely or otherwise) designed to obtain information using equipment producing "electromagnetic, acoustic and other emissions, or information derived from or related to such equipment" [132], [133]. Generally speaking, equipment interference is used to obtain information from equipment.

2) INVESTIGATORY POWERS ACT

Part 5 of the Investigatory Powers Act provides the primary legal framework for LEAs and intelligence services in the UK to obtain data from devices by interfering with associated electronic equipment [134]. The Act allows for the interference with electronic equipment such as computers and smartphones to obtain communications, equipment data, or other information [135].

In the UK government guidance, ''equipment'' is defined as any device producing ''electromagnetic, acoustic or other emissions and any device capable of being used in connection with such equipment'' [136]. This definition covers computers and smartphones as well as tablets and other network devices [136]. Cables, wires, USB storage devices, CDs, and hard disk drives are also covered because they can also produce electromagnetic emissions [136].

In this context, equipment interference can include many different hacking techniques (e.g., malware, spyware, and key loggers) and covers both physical and remote interference, including covertly downloading data from a physically compromised device or installing malware onto a device through the network for the purposes of extracting information [136].

E. THE UNITED STATES

Although there is no clear legislation regarding the use of government hacking techniques in the United States, Rule 41 of the Federal Rules of Criminal Procedure has been interpreted as authorizing LEAs to use search and seizure warrants to apply ''remote access'' in investigations [41], [106], [137]. An important amendment added to Rule 41 in 2016 [138]–[140] expands the reach of the act under two circumstances: when a suspect has hidden a device using technological means, and when the LEA can identify devices located in multiple jurisdictions. These amendments make it possible for LEAs to obtain judicial warrants to search for computers located in unknown or multiple locations [141]. Such remote access warrants can be used to search storage media and seize or copy stored information [142], through the use of remote access, which can be used not only to obtain a suspect's IP address but also to activate microphones in cell phones or laptops to record the suspect's conversations [141].

IV. SUMMARY OF DISCLOSED GOVERNMENT HACKING EVENTS AND TECHNIQUES

National security concerns generally dictate that techniques and methods used in government hacking are kept secret, although some aspects of these programs and activities have surfaced in the media. In this section, we summarize some of the better-known government hacking events that have taken place in recent years.

A. DISCLOSED GOVERNMENT HACKING TECHNIQUES USED BY THE FBI

The earliest disclosed case of the use by the U.S. Federal Bureau of Investigation (FBI) of government hacking tools took place in 1999 [40], [45], [143] and involved the use of key logger software [45], which was installed physically by an FBI agent to record keystrokes entered into a suspect's computer. Through this measure, the agent was able to find a Pretty Good Privacy (PGP) key to the suspect's files, which were then decrypted [45]. The agent subsequently used a new key logger software application called the Magic Lantern, which was installed via social engineering tricks and software vulnerabilities [144]–[146]. This use of more sophisticated software indicates that the FBI has previously used government hacking tools remotely. Around the same time, the ''Carnivore'' system was placed on the backbones of several ISPs as a traffic sniffer [45].

In 2007, the FBI installed a Computer Internet Protocol Address Verifier (CIPAV) onto an anonymous suspect's computer to obtain information including their IP/MAC address, a list of open TCP/UDP port numbers, running programs, operating system data, the current username, and visited websites [45], [143]. This government hacking tool could also be used to covertly activate microphones and record conversations [147], extract stored files, photographs, and e-mails, and collect real-time images by activating cameras on the suspect's device [148], [149]

The FBI used a tool called the ''watering hole attack'' in a child pornography website investigation case [45], [147]. This method involves embedding spyware in web pages and collecting IP addresses and other identifying information from visitors. The FBI also applied zero-day exploits in the case [150].

B. HACKING TEAM

HackingTeam is an Italian software company that sells government hacking tools to organizations around the world including militaries, law enforcement agencies, intelligence services, and corporations [151].

In 2015, the company was hacked and the unknown hackers subsequently uploaded approximately 400 GB of data to BitTorrent [152]. The disclosed information and files, which include emails, documents, source codes, and lists of current and past clients, was subsequently published on WikiLeaks [153].

Products known as Remote Control Systems (RCS), which include ''Da Vinci'' and ''Galileo'' platforms, have been shown to be able to infiltrate desktop computers, laptops, and smartphones via a number of zero-day exploits in several common applications such as Adobe Flash, Internet Explorer, and mobile operating systems, allowing a suspect's systems to be remotely controlled without their knowledge [154]. RCS is used to monitor communication between internet users, decipher encrypted emails, record VoIP communications such as Skype, secretly access stored data and photos, and activate microphones and cameras on suspects' devices [155].

C. GAMMA GROUP

Gamma Group is a joint German-UK government malware company that produces the ''FinFisher'' suite, which has been sold to a number of governments and police agencies [156]–[158]. In their first Spy Files release in 2011, WikiLeaks shared documents relating to the use of FinFisher in government hacking products employing remote monitoring, infection, tactical solutions, and training courses [159]. In 2014, Gamma Group was hacked by an anonymous hacker who disclosed 40 GB of internal documents [160], [161]

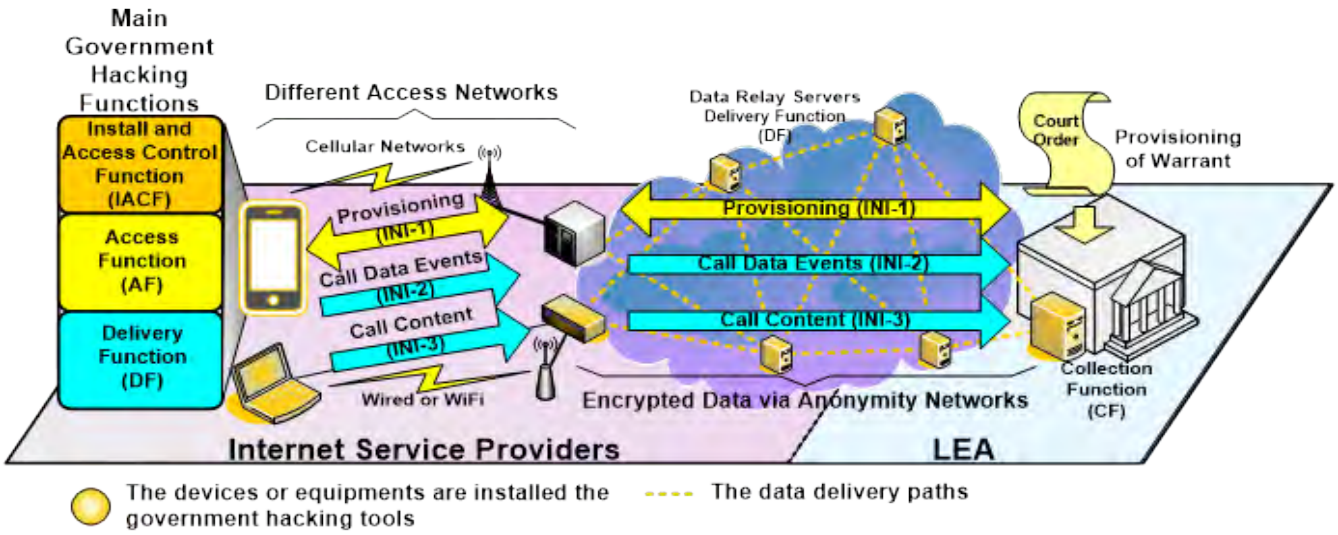

FIGURE 2. Generic view of government hacking architecture.

confirming that the company sold government hacking tools and performed related technical consulting.

Government hacking products developed by Gamma Group have been inserted into well-known commercial software with the goal of applying common hacking techniques such as Trojan horse, malware, social engineering and security exploits to infect the operating systems of suspects' computers and smartphones [162], [163].

The company's products, which can be applied under different situations, include FinIntrusion Kit, Fin USB Suite, FinFireWire, FinSpy, FinSpy Mobile, and FinFly [USB, LAN, Web, and ISP] [162]. Gamma Group also claims that their products can bypass antivirus systems and access data without detection [162].

FinFisher can intercept encrypted communications, access stored data, perform live surveillance, remote forensics, and location tracking, and extract files from a suspect's computer and devices [162]. Its main functionalities are similar to those of the HackingTeam RCS, which we discussed previously. Analysis by a security company revealed that FinFisher was quite active as of 2017 and that its latest version was applying the ''man-in-the-middle'' technique to infect suspects' devices [164].

D. VAULT 7

WikiLeaks also disclosed the existence of the controversial US government hacking suite named ''Vault 7,'' which they claimed had been leaked by the Central Intelligence Agency (CIA) in 2017 [165]. The apparent coverage of the agency's government hacking suites was indicated by the coverage of Vault 7 component ''Year Zero,'' which contained 8,761 documents and files [165]. The focus of the suite on common operating systems, smartphones, smart TVs, networks devices, and commercial software suggests that CIA has previously used a broad variety of hacking tools, including Trojan horse, malware, security exploits, and remote monitoring systems.

Based on the released descriptions of the disclosed suites, one has the ability to transform a smart TV into a covert microphone [166], while another can execute code on peripheral devices used with major brand laptops or desktops [167]. The suites also apply common smartphones hacking tools [165] through which infected phones can be instructed by the agency to relay a user's geolocation, audio, and text communications and activate the phone's camera and microphone [165]. These tools have been used by CIA agents to intercept calls and messages through the hacking of smartphones prior to their encryption.

E. COMMON FUNCTIONALITIES OF GOVERNMENT HACKING TOOLS

The preceding review revealed the use of government hacking tools by several countries. Although the tools used may be different, their main functionalities are essentially the same. Such tools are generally used to obtain a suspect's communications and data. Conceptually, they are similar to LI and digital forensics equipment except that they are applied in the execution of hacking techniques. For example, the main difference between LI and government hacking is that, in the latter, the ''access'' and ''delivery'' functions are moved from the telecommunication service network to the suspect's device, as shown in Figure 2; accordingly, the LEA must install their tool into a suspect's device. In addition, it is very important to carefully delineate the conditions under which the tool can be accessed, and it is vital to confine the agency to only accessing specifically authorized communication or data. In the following, we explain the common functionalities and workflow of government hacking.

1) INSTALL AND ACCESS CONTROL FUNCTION

The install and access control function (IACF) is used to set up a government hacking tool in a suspect's device and to control the tool's access permissions. This function must

run in the background of the suspect's device while waiting to receive and execute commands from the LEA; as such, it is the most important and difficult to implement of all functions. The IACF often applies several exploits or vulnerabilities to bypass or break down the security mechanism of the target device in installing the tool. In general, there are three common methods for IACF implementation: physical, social engineering, and remote (Table 5). To use physical installation, the LEA must obtain the suspect's device to load the relevant tools directly from a cable or storage media. Of course, the device must be installed and accessed covertly, and doing so under actual field conditions remains a difficult challenge that has led to the introduction of social engineering and remote installation methods.

TABLE 5. Common IACF installation methods [183].

Installation Methods	Description
Physical	Tool is installed on the device either through USB/optical disc storage or memory card. However, the LEA agent must obtain the device from the suspect.
Social Engineering	SMS/MMS/E-mail/IM is used to send a sophisticated message with a malicious link or malware to the suspect. Once the suspect clicks the link or opens the file, the tools will be downloaded and activated on the device automatically.
Remote	The tool is installed without the use of physical or social engineering methods. Typically, the LEA uses high-order zero-day exploits or vulnerabilities to infect the device. One disclosed techniques uses a "Network Injector" to monitor all HTTP connections from the suspect and then attempt to inject the tool onto the device.

The social engineering installation method involves sending the suspect a sophisticated message containing a malicious link or malware. Once the suspect clicks on the appropriate link or file, the tools are downloaded and activated in the device. Some government hacking tools will use specific document spoofs that the suspect may even install himself. By contrast, under the remote installation approach the suspect does not have to click anything; instead, events such as visits to a specific website are used to trigger automatic tool downloading and activation

The other main task of IACF is permission control. This function is used to ensure that only authenticated agents of the LEA can utilize the tools to access a targeted device while confining the access permissions to communication and data that are provided to the LEA. Although government hacking tools employ hacking techniques, the LEA is not technically supposed to act as a conventional "hacker," and agents should only be able to access communications and data within an authorized range.

2) ACCESS FUNCTION

Once the government hacking tool has been mounted in the suspect's device, it begins collecting all communications and data that the LEA has authorized. The access function (AF) plays an important in this task by implementing the capacities listed in Table 6 in a manner similar to the use by enterprises of mobile device management (MDM) software to perform forensic tasks [168], [169]. Typically, there will be a few protection mechanisms in an individual application or device that will block the AF from obtaining data; in such cases, the IACF must be used to obtain, for example, root privileges on the device [170] to enable the AF to function. Some applications use secure socket layers (SSLs) or transport layer security (TLS) to encrypt communications [171], [172]. To overcome this, a common hacking technique called the "man-in-the-middle" attack [171], [173] can be used to break down SSL/TLS mechanisms by moving the AF from the device to network equipment such as a rogue Wi-Fi hotspot or a fake base station [174]–[176]. In some cases, potential security issues in a mobile network can be used to help the AF bypass the security mechanisms [177]–[180].

3) DELIVERY FUNCTION

Once the tools have collected the data, they must be stored in the device temporarily in an encrypted format while waiting for an opportune moment for covert transmission to the LEA via relay servers [162] or hidden services [181], [182]. This is the main task of the delivery function, which must keep the suspect from becoming aware of abnormal transmissions from their device.

4) COLLECTION FUNCTION

Data sent back to the LEA will arrive in a disordered state, requiring the use of a collection function (CF) to decrypt and separate data from respective suspects. In many cases, individual LEA agents can only view data on a specific suspect whom they are authorized to investigate. This function differs from the other three functionalities in that it is located on the LEA side.

5) THE GENERAL WORKFLOW OF GOVERNMENT HACKING TOOLS

Government hacking tools apply different methods and are used under different scenarios. Although such tools do not have standard usage processes, workflows, or template-based solutions, it is possible to summarize some common steps as a generalized workflow. Here, we describe the initial and terminating workflows for government hacking tool usage, which are shown in Figures 3 and 4, respectively, and describe the role of the functionalities in the workflows.

The initial workflow, which involves the LEA setting up the government hacking tool in the suspect's device, is given as follows:

Step 1: Upon receiving a court order to authorize the surveillance of a suspect using a government hacking tool, the LEA must first gather and analyze the target device's information (e.g., its brand, model, operating system type, and installed applications).

Step 2: The LEA chooses a suitable tool for the device in question and then validates the tool in a laboratory environment.

TABLE 6. Summary of well-known Government Hacking events and their capacities.

Name Disclosure year	FBI Since 1999	HackingTeam Since 2015	Gamma Group Since 2014	Vault 7 Since 2017
Names of the primary disclosed tools	Carnivore, Magic Lantern, Computer Internet Protocol Address Verifier, Watering Hole Attack	Remote Control Systems (Including the Da Vinci and Galileo platforms)	Finfisher (Including FinIntrusion Kit, Fin USB Suite, FinFireWire, FinSpy, FinSpy Mobile, FinFly [USB, LAN, Web, and ISP])	Dark Matter, Marble Framework, Grasshopper, Hive, Weeping Angel, Scribbles, Archimedes, AfterMidnight, Athena, Pandemic, Cherry Blossom, Brutal Kangaroo, Elsa, OutlawCountry, BothanSpy, Highrise, UCL/Raytheon, Imperial, Dumbo, CouchPotato, ExpressLane, Angelfire, Protego
Main capacities of the tools	Intercept traffic Keylogger Obtain IP and MAC address Obtain OS, usernames and visited website information List opening ports and running programs Activate microphones and camera Extract stored data For common computer and mobile device OS	Intercept traffic Chat/IM/SMS/MMS messages, E-mail and VoIP Keylogger Obtain IP and MAC address Obtain OS, usernames, location (GPS or Cell) and visited website information Activate microphones and camera (screenshot) Extract stored data For common computer and mobile device OS	Intercept traffic Chat/IM/SMS/MMS messages, E-mail and VoIP Keylogger Obtain IP and MAC address Obtain OS, usernames, location (GPS or Cell) and visited website information Activate microphones and camera (screenshot) Extract stored data For common computer and mobile device OS	Intercept traffic Chat/IM/SMS messages, E-mail and VoIP Obtain IP and MAC address Obtain usernames, location (Wi-Fi AP aid) Activate microphones and camera Extract stored data For common computer and mobile device OS

Steps 3–5: The LEA determines whether the individual functions are matched to the device. Any mismatched function should be modified or redeveloped.

Step 6: The tool is installed on the suspect's device, and the availability of the IACF and AF is verified.

Step 7: The parameters of the tool (e.g., the duration of the surveillance order, the interval and trigger events for data return, and the types of data authorized for collection) are set, and the availability of the DF and CF is verified. The LEA can now use the tool to access data from the suspect.

The terminating workflow involves de-installation of the government hacking tool by the LEA. This workflow is as follows:

Step 1: Upon expiration of the surveillance period or receipt of notification by the LEA of a termination order, the LEA cases to use the tool to access and retrieve data from the device.

Step 2: The LEA must delete temporarily stored data from the device.

Step 3: The AF and DF are terminated and removed from the device.

Step 4: The IACF is terminated and then removed from the device. During Steps 3 and 4, the device will occasionally automatically restart or shut down, which can alert the suspect to the presence of surveillance activities. In some cases, the suspect is required to authorize the removal of the tool [183].

Step 5: After the LEA terminates the device functions, it must disable the CF for the device in their own system. Once this is done, the LEA has fully terminated the government hacking tool.

V. OPEN CHALLENGES AND FUTURE DIRECTIONS

Although government hacking provides the potential for new tactics and opportunities for LEA investigation, it also presents novel security and privacy impacts. Many aspects of government hacking require further research, and a government wishing to use hacking techniques in good faith should discuss such subjects in public. This section highlights the technology and management challenges and future directions of government hacking.

A. ENCRYPTION

Encryption is the major reason for the application of government hacking techniques. The development of high-performance devices has made it easier to apply complex new encryption algorithms on smartphones and tablets, and most new applications now feature embedded and frequently updated encryption mechanisms. Thus, breaking down and bypassing encrypted mechanisms to obtain a suspect's communications or data in a timely manner is a very challenging problem.

A popular anonymity network, the Onion Router (Tor) [181], can access the Internet with encryption and should also be discussed here. Once the network traffic is routed into the Tor network, the traffic passes through at least three different Tor nodes before reaching the destination server. The initial packets are encrypted, and each Tor node

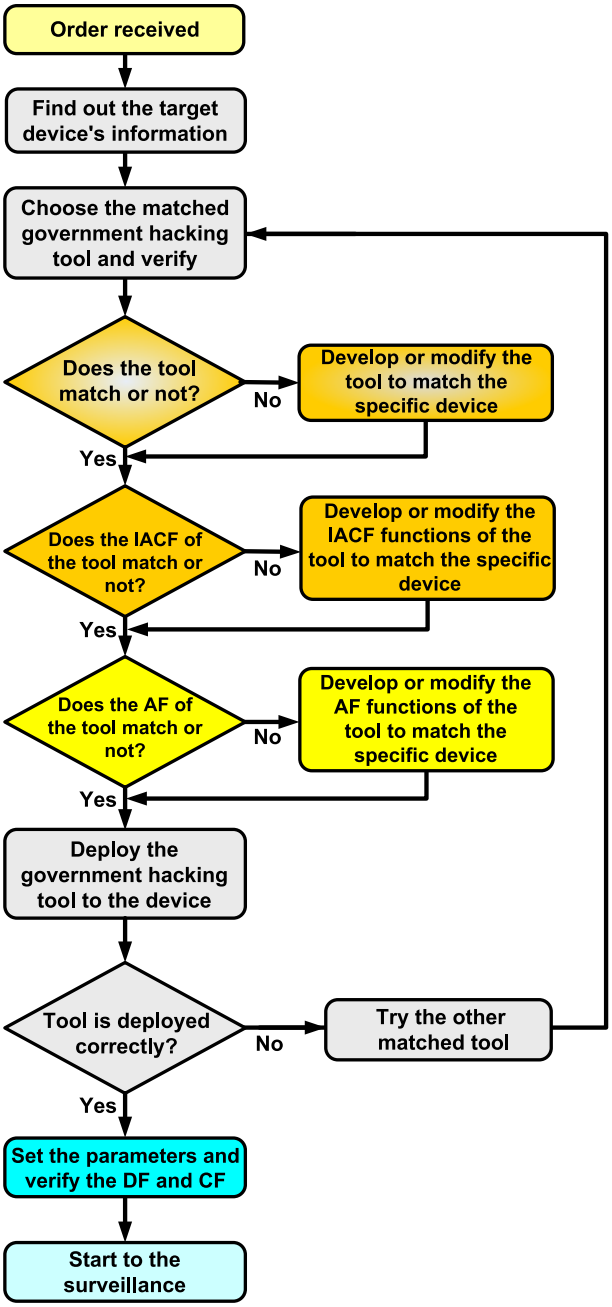

FIGURE 3. Initial workflow for using government hacking tool.

along the link only decrypts the layer that contains the information necessary to route the packet. The traffic is encrypted between each client to the exit node. This means that there is no separate Tor node to identify the exact source and destination address from the traffic at the same time. In addition, the nodes on the entire path can often be changed. The hidden service utilizes these properties of the Tor network to provide anonymity to websites and other servers [182]. Many platforms with illegal content and transactions have been hidden in this service. Because the LEA cannot obtain detailed information on the clients and servers, launching government hacking activities becomes difficult.

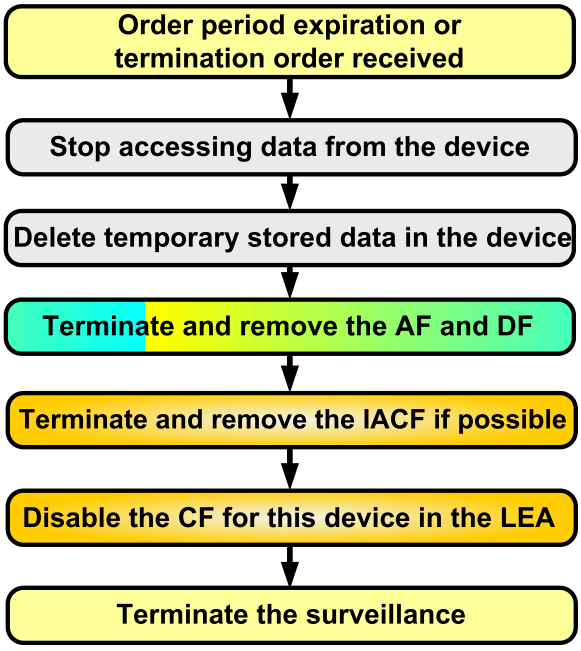

FIGURE 4. Terminating workflow for using government hacking tool.

B. VARIETIES OF DEVICES AND APPLICATIONS

In the previous section, it was shown that government hacking methods and techniques are highly driven by the design of the devices, operating systems, and applications that they must access. However, there is a wide variety of types and brands of devices that consumers can choose from on the market. Devices have different hardware configurations (with variations even within a given model), customized operating systems, and applications, and there is no generic hacking approach that can be adopted by government agencies to reproduce the standardized LI solutions that were used in the past. Instead, each tool and technique must be somewhat tailored to the target device and application.

C. COST

The need for tool providers to develop customized tools for each LEA to ensure individual compatibility with different devices, applications, and encryption mechanisms means that such tools are costly. Frequent updates by providers of operating systems and software also add to the cost of tool development. Reducing the large expenses that LEAs must pay to tool providers for development and maintenance is, therefore, an important avenue of research.

D. OPERATING SECURITY

The security requirements of government hacking tools are similar to those of conventional LI. Under general interception standards, for example, no communicating party should be able to discriminate between intercepted and non-intercepted states [65] and the operating facilities and quality of other services should not be altered as the result of interception measures [65]. In some cases,

the vestiges of government hacking can be found by anti-virus software or network forensic tools and programs [164], [184]–[186]. To avoid discovery of such pieces of "evidence," government hacking tools need to incorporate approaches such as data encryption, hidden anti-forensics, and transmit-ability via anonymity networks and should be capable of passing the newest anti-virus suites and firewalls. In addition, tool providers need to ensure that collected data are stored securely and cannot be accessed by unauthorized users.

E. PRIVACY AND POLICY CONTROL

In a conventional LI operation, a wiretapping warrant can only be used to intercept a named suspect's communications and cannot authorize access to additional data or the activation of unauthorized functions such as viewing contacts, stored photos, or documents, accessing GPS information, or turning on the camera and/or microphone. However, once an LEA has applied hacking tools to a suspect's computer or device, concerns arise as to whether the LEA will retrieve stored data or activate functions without supervision. The issue of confining the capacity of government hacking tools to the areas authorized under the warrant and developing overseeing mechanisms remains an important area of inquiry. The questions regarding three topics relating to this issue—legally permitted range, tool design and manufacture, and management and oversight mechanism—are discussed as follows.

- Legally permitted range: This involves questions regarding the planning of the legal requirements and procedures of government hacking usage. Human rights are heavily impacted during government hacking activities by a state. What safeguards of the legal framework should be adopted to resolve this issue? Is it necessary to add more stringent regulations for government hacking warrants? In addition to terrorism, cyber-attacks, threat-to-life, and child sexual exploitation, what kinds of serious crime or national security cases can also be investigated by government hacking? What situations and legal conditions should deal with a warrant that can access the partial or full personal information? Are the government hacking technologies matched to these situations and conditions? What are their requirements and limitations? How should obtained data unrelated to an LEA's investigation be processed? How should the tool be applied to suspects within a local jurisdiction or suspects in a foreign region?
- Tool design and manufacture: This involves the determination of whether an unauthorized function is presented in a tool while ensuring that the tool makes necessary modifications to a suspect's storage data and related parameters with minimal impact. This raises questions including: how can it be ensured that, upon warrant expiration, the tool automatically becomes invalid and removable from the suspect's device; is the tool's operation in line with LEA expectations; should engineers and legal staffs review the source code together; and how can it be ensured that a monitored individual does not become suspicious of the use of the tool?
- Management and oversight mechanism: This involves questions as to whether and how a tool and its operator can be verified by a third-party certifying authority, and the importance of designing and managing a tool operating procedure that prevents operator abuse. This raises questions such as: is it necessary to give an independent institution outside of the LEA the responsibility for researching, developing, and manipulating tools?; is it necessary to designate yet another institution to audit tool usage?; and, if so, how should this audit mechanism operate?

F. VULNERABILITY DISCLOSURE

Zero-day exploits or vulnerabilities comprise the core of government hacking tools because they enable the IACF to "open the door" and install the tool into the suspect's equipment. An LEA that develops a zero-day exploit will of course want to retain it, and intelligence and law enforcement agencies are naturally averse to the disclosure of their sources and methods. However, such vulnerabilities can have significant economic, privacy, and national security implications. If a particular zero-day represents a particularly high risk or is widespread in critical infrastructure, the question arises as to whether the LEA should disclose it.

The U.S. government has introduced a procedure called the "Vulnerabilities Equities Process" (VEP) [187] to determine which zero-day exploits or vulnerabilities discovered by government agencies in computers, devices, or equipment can be released to security companies for patching and which are to remain classified for potential operational use by intelligence or LEAs [188]. This process runs the risk of discovery and covert exploitation in bad faith of classified exploits or vulnerabilities, and some researchers have advocated for the open disclosure of all exploits [189]. The design of mechanisms to balance the security of equipment with the availability of exploits and vulnerabilities remains a significant challenge.

G. STANDARDIZATION AND COOPERATION AGREEMENT

Digital forensic tools must be verified to guarantee that they consistently produce accurate and objective test results [190], [191], and the identification, collection, acquisition, and preservation of digital evidence is becoming standardized [192]. Using government hacking tools to collect data from a suspect's devices is similar to a remote forensics operation and, as in forensics cases, obtained data should be well protected.

Governments should therefore follow the example of the digital forensics tool industry [190] in establishing a methodology for testing government hacking tools through the development of general tool specifications, test criteria, conditions, cases, procedures, and hardware. Developing a full standard for testing procedures for government hacking tools to

avoid legal challenges is another important future avenue of research.

Moreover, government hacking technologies can be used through the Internet on a global scale, irrespective of national and transnational borders. International cooperation agreements, such as the Convention on Cybercrime, should include government hacking activities to avoid sovereignty violation that can lead to international conflict.

H. WEAPONS PROLIFERATION

Like viruses, Trojans, and other devastating weapons of the digital world, government hacking tools are, in general, simply code. Such tools can be copied rapidly and easily without additional cost or effort, and their developers and users typically have excellent skillsets for bypassing tracing, making proliferation very difficult to avoid. Once such tools have been stolen, they can end up in the hands of criminals or terrorists [193]. This makes it vital to develop methods for designing appropriate functions and mechanisms to avoid the abuse of government hacking tools by unauthorized users.

VI. CONCLUSION

Applying government hacking technologies in the service of public security remains a pressing concern for governments and the people they serve. In this paper, we provided background on the state-of-the-art in communication surveillance. After briefly highlighting the current state of LI, we reviewed regulations, standards, and the going dark challenge, which has induced many governments to employ hacking-based surveillance techniques and laws to intercept communication by suspects. We summarized the regulatory frameworks of five countries that have applied government hacking and reviewed well-known and important government hacking events deduced from disclosed documents and files. Finally, we presented and discussed the open challenges and future directions of government hacking.

REFERENCES

[1] A. Joel, "Telecommunications and the IEEE Communications Society," *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 6–162, May 2002.

[2] S. Bhatnagar and S. Ganguly, *VoIP: Wireless, P2P and New Enterprise Voice Over IP*. Chichester, U.K.: Wiley, 2008.

[3] W. Diffie and S. Landau, "Communications surveillance: Privacy and security at risk," *Commun. ACM*, vol. 52, no. 11, pp. 42–47, 2009. [Online]. Available: https://cacm.acm.org/magazines/2009/11/48445-communications-surveillance-privacy-and-security-at-risk/fulltext

[4] J. J. Roberts. (Nov. 30, 2016). Rule 41 Grants New Hacking Powers to FBI. Fortune. Accessed: Dec. 30, 2017. [Online]. Available: http://fortune.com/2016/11/30/rule-41/

[5] K. Baker. (Mar. 13, 2016). Police and Spy Agencies to Get Powers to Hack Into Your Mobile Phone. Daily Mail. Accessed: Dec. 30, 2017. [Online]. Available: http://www.dailymail.co.uk/news/article-3490278/Police-spy-agencies-powers-hack-mobile-phone.html

[6] Deutsche Welle. (Feb. 22, 2016). *German Government to Use Trojan Spyware to Monitor Citizens*. Accessed: Dec. 30, 2017. [Online]. Available: http://www.dw.com/en/german-government-to-use-trojan-spyware-to-monitor-citizens/a-19066629

[7] S. Landau, "Security, wiretapping, and the Internet," *IEEE Security Privacy*, vol. 52, no. 11, pp. 26–33, Dec. 2005. [Online]. Available: http://ieeexplore.ieee.org/document/1556533/

[8] The Federal Communications Commission. *Communications Assistance for Law Enforcement Act*. Accessed: Dec. 27, 2017. [Online]. Available: https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[9] L. Kleinrock, "History of the Internet and its flexible future," *IEEE Wireless Commun.*, vol. 15, no. 1, pp. 8–18, Feb. 2008.

[10] P. V. Mockapetris, "Telephony's next act," *IEEE Spectr.*, vol. 43, no. 4, pp. 28–32, Apr. 2006. [Online]. Available: http://ieeexplore.ieee.org/document/1611758/

[11] J. Middleton, "Voice over IP: Setting phone service free," *IEEE Spectr.*, Dec. 2010. Accessed: Dec. 27, 2016. [Online]. Available: https://spectrum.ieee.org/telecom/internet/voice-over-ip-setting-phone-service-free

[12] The Advisory Committee on International Communications and Information Policy. *Voice Over Internet Protocol: Status and Industry Recommendations*. Accessed: Dec. 25, 2017. [Online]. Available: https://2001-2009.state.gov/e/eeb/adcom/47331.htm

[13] S. Cherry, "The end of the public phone network," *IEEE Spectr.*, Dec. 2012. Accessed: Dec. 27, 2017. [Online]. Available: https://spectrum.ieee.org/podcast/telecom/internet/the-end-of-the-public-phone-network

[14] *Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD)*, document ETSI TR 101 567, 2016.

[15] *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP Delivery; Part 1: Handover Specification for IP Delivery*, document ETSI TR 101 567, 2016.

[16] *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP Delivery; Part 5: Service-Specific Details for IP Multimedia Services*, document ETSI TS 102 232-5, 2017.

[17] *Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub—Part 2: Streamed Multimedia Services*, document ETSI TS 101 909-20-2, 2005.

[18] *Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 20: Lawful Interception; Sub—Part 1: CMS Based Voice Telephony Services*, document ETSI TS 101 909-20-1, 2005.

[19] *PacketCable Electronic Surveillance Delivery Function to Collection Function Interface Specification*, CableLabs document PKT-SP-ES-DCI-C01-140314, 2014.

[20] (Apr. 2003). *Lawfully Authorized Electronic Surveillance, ATIS/TIA J-STD-025-A*. Accessed: Dec. 30, 2017. [Online]. Available: https://www.atis.org/docstore/product.aspx?id=11438

[21] *Lawfully Authorized Electronic Surveillance (LAES) for Voice Over Packet Technologies in Wireline Telecommunications Networks*, ATIS Standard PP-1000678.2006, 2006.

[22] FBI National Press Office. (2006). *Statement of FBI Assistant Director Kerry E. Haynes, Operational Technology Division, on Today's Court Ruling on VOIP*. [Online]. Available: https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-of-fbi-assistant-director-kerry-e.-haynes-operational-technology-division-on-today2019s-court-ruling-on-voip

[23] FBI National Press Office. (Sep. 7, 2004). *Federal Bureau of Investigation Calls Cablelabs Release of Its Packetcable Electronic Surveillance*. Accessed: Dec. 27, 2017. [Online]. Available: https://archives.fbi.gov/archives/news/pressrel/press-releases/federal-bureau-of-investigation-calls-cablelabsae-release-of-its-packetcabletm

[24] (2005). *The Advisory Committee on International Communications and Information Policy, Voice Over Internet Protocol: Status and Industry Recommendations*. Accessed: Dec. 27, 2017. [Online]. Available: https://2001-2009.state.gov/e/eeb/adcom/47331.htm

[25] M. Dargue and W. Wadsworth. (2013). *Over the Top Operator Threat and Opportunity*. [Online]. Available: https://www.cartesian.com/wp-content/uploads/2015/07/OTT-Operator-Threat-and-Opportunity_Cartesian_Feb2013.pdf

[26] K. P. O'Hara, M. Massimi, R. Harper, S. Rubens, and J. Morris, "Everyday dwelling with WhatsApp," in *Proc. 17th ACM Conf. Comput. Supported Cooper. Work Soc. Comput. (CSCW)*, vol. 14, 2014, pp. 1131–1143, [Online]. Available: http://dl.acm.org/citation.cfm?doid=2531602.2531679

[27] V. Caproni. (Feb. 2011). *FBI—Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*. Accessed: Dec. 30, 2017. [Online]. Available: https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies

[28] lectronic Frontier Foundation. *Going Dark: FOIA Documents—Release 1, Part 1 Electronic Frontier Foundation*. Accessed: Dec. 29, 2017. [Online]. Available: https://www.eff.org/document/fbi-going-dark-foia-documents-release-1-part-1

[29] I. Godlovitch, B. Kotterink, J. S. Marcus, P. Nooren, J. Esmeijer, and A. Roosendaal, "Over-the-Top (OTTs) players: Market dynamics and policy challenges," Eur. Parliament's Committee Internal Market Consum. Protection (IMCO), Brussels, Belgium, Stud. Rep. PE 569.979, Dec. 2015.

[30] J. Corpuz. (Mar. 9, 2017). Best VoIP Apps for Your Desktop. Tom'S Guide. Accessed: Dec. 30, 2017. [Online]. Available: https://www.tomsguide.com/us/pictures-story/519-best-voip-apps.html#s10

[31] M. Casserly. (Sep. 11, 2017). Best Free Email Services 2017. Tech Advisor. Accessed: Dec. 30, 2017. [Online]. Available: https://www.techadvisor.co.uk/feature/internet/best-free-email-services-for-2017-3613837/

[32] J. Corpuz. (Dec. 8, 2017). Best Messaging Apps. Tom's Guide. Accessed: Dec. 30, 2017. [Online]. Available: https://www.tomsguide.com/us/pictures-story/654-best-messaging-apps.html#s27

[33] Statista. (Mar. 2017). *App Stores: Number of Apps in Leading App Stores 2017*. Accessed: Dec. 30, 2017. [Online]. Available: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[34] J. Corpuz. (Oct. 16, 2017). *Best Encrypted Messaging Apps. Tom's Guide*. Accessed: Dec. 30, 2017. [Online]. Available: https://www.tomsguide.com/us/pictures-story/761-best-encrypted-messaging-apps.html

[35] S. E. Coull and K. P. Dyer, "Traffic analysis of encrypted messaging services: Apple imessage and beyond," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 5–11, Oct. 2014. Accessed: Dec. 30, 2017. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2677046.2677048

[36] M. Conti, L. V. Mancini, R. Spolaor, and N. V. Verde, "Analyzing Android encrypted network traffic to identify user actions," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 114–125, Jan. 2016. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7265055/

[37] A. Azfar, K.-K. R. Choo, and L. Liu, "Android mobile VoIP apps: A survey and examination of their security and privacy," *Electron. Commerce Res.*, vol. 16, no. 1, pp. 73–111, Mar. 2016. Accessed: Dec. 30, 2017. [Online]. Available: http://link.springer.com/10.1007/s10660-015-9208-1

[38] Statista. *Mobile Messenger Apps—Statistics & Facts*. Accessed: Dec. 30, 2017. [Online]. Available: https://www.statista.com/topics/1523/mobile-messenger-apps/

[39] S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, "Going bright: Wiretapping without weakening communications infrastructure," *IEEE Security Privacy*, vol. 11, no. 1, pp. 62–72, Jan. 2013. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/6357177/

[40] K. Zetter. (May 15, 2016). *Everything We Know About How the FBI Hacks People*. Accessed: Dec. 30, 2017. [Online]. Available: https://www.wired.com/2016/05/history-fbis-hacking/

[41] Stanford Center for Internet and Society. *Government Hacking*. Accessed: Dec. 30, 2017. [Online]. Available: http://cyberlaw.stanford.edu/our-work/projects/government-hacking

[42] N. Anderson. (Jun. 1, 2012). Confirmed: US and Israel Created Stuxnet, Lost Control of it. Ars Technica. Accessed: Dec. 30, 2017. [Online]. Available: https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

[43] G. Moody. (Feb. 25, 2016). German Police Can Now Use Spyware to Monitor Suspects. Ars Technica. Accessed: Dec. 30, 2017. [Online]. Available: https://arstechnica.com/tech-policy/2016/02/german-police-can-now-use-spying-malware-to-monitor-suspects/

[44] O. S. Kerr and S. D. Murphy, "Government hacking to light the dark Web: What risks to international relations and international law?" *Stanford Law Rev. Online*, vol. 70, pp. 58–69, Jul. 2017. Accessed: Dec. 30, 2017. [Online]. Available: https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/07/70-Stan.-L.-Rev.-Online-58-Kerr-Murphy.pdf

[45] S. Quinlan and A. Wilson. (Sep. 2016). A Brief History of Law Enforcement Hacking in the United States. New America. Accessed: Dec. 30, 2017. [Online]. Available: https://na-production.s3.amazonaws.com/documents/History_Hacking.pdf

[46] D. L. Sobel, "Will Carnivore devour online privacy?" *Computer*, vol. 34, no. 5, pp. 87–88, May 2001. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/920616/

[47] G. Lawton, "Invasive software: Who," *Computer*, vol. 35, no. 7, pp. 15–18, Jul. 2002. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/1016895/

[48] L. D. Paulson, "Key snooping technology causes controversy," *Computer*, vol. 35, no. 3, p. 27, Mar. 2002. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/989923/

[49] M. Blaze, "Taking surveillance out of the shadows," *IEEE Security Privacy Mag.*, vol. 7, no. 5, pp. 75–77, Sep. 2009. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/5280139/

[50] H. Berghel, "Through the PRISM darkly," *Computer*, vol. 46, no. 7, pp. 86–90, Jul. 2013. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/6576770/

[51] L. DeNardis, "The Internet design tension between surveillance and security," *IEEE Ann. History Comput.*, vol. 37, no. 2, pp. 72–83, Apr. 2015. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7116471/

[52] S. M. Bellovin, M. Blaze, and S. Landau, "Insecure surveillance: Technical issues with remote computer searches," *Computer*, vol. 49, no. 3, pp. 14–24, Mar. 2016. Accessed: Dec. 30, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7433349/

[53] S. Landau, "The real security issues of the iPhone case," *Science*, vol. 352, no. 6292, pp. 1398–1399, Jun. 2016. [Online]. Available: http://www.sciencemag.org/cgi/doi/10.1126/science.aaf7708

[54] *Lawfully Authorized Electronic Surveillance*, document ATIS/TIA J-STD-025-B, Jul. 2006. Accessed: Dec. 30, 2017. [Online]. Available: https://www.atis.org/docstore/product.aspx?id=22579

[55] *Lawful Interception Requirements*, document 3GPP TS 33.106 V14.1.0, (Release 14), Jun. 2017. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2265

[56] *Lawful Interception Architecture and Functions*, document 3GPP TS 33.107 V14.4.0 (Release 14), Sep. 2017. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2266

[57] *Handover Interface for the Lawful Interception*, document 3GPP TS 33.108 V14.2.0, Sep. 2017. [Online]. Available: ftp://ftp.3gpp.org/Specs/2017-12/

[58] C. Rizzo and C. Brookson, "Lawful interception," ETSI, Sophia Antipolis, France, White Paper, 2015, pp. 31–33. Accessed: Jan. 2, 2018. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf

[59] ETSI. *Lawful Interception Standards*. Accessed: Dec. 30, 2017. [Online]. Available: http://www.etsi.org/technologies-clusters/technologies/lawful-interception

[60] C. Sharp, B. Foster, and F. Baker, *Cisco Architecture for Lawful Intercept in IP Networks*, document IETF RFC 3924, 2004. Accessed: Jan. 3, 2018. [Online]. Available: https://tools.ietf.org/html/rfc3924

[61] P. Hoffmann and K. Terplan, "Legal and technical standards for lawful intercepts," in *Intelligence Support Systems: Technologies for Lawful Intercepts*. New York, NY, USA: Auerbach, 2006, pp. 61–94.

[62] *Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic*, Standard ETSI TS 101 671 V.3.13.1, Nov. 2015. Accessed: Dec. 31, 2017. [Online]. Available: http://www.etsi.org/standards-search

[63] *Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic*, Standard ETSI ES 201 671 V3.1.1, May 2007. Accessed: Jan. 3, 2018. [Online]. Available: http://www.etsi.org

[64] G. Amato, "Lawful intercept management modules and methods for LI-configuration of an internal interception function in a cloud based network," U.S. Patent 2016 0 112 261 A1, Apr. 21, 2016. Accessed: Jan. 1, 2018. [Online]. Available: http://www.freepatentsonline.com/y2016/0112261.html

[65] *Lawful Interception (LI); Requirements of Law Enforcement Agencies*, Standard ETSI TS 101 331 V1.5.1, Mar. 2017. Accessed: Jan. 1, 2018. [Online]. Available: http://www.etsi.org/standards-search

[66] Australian Department of Home Affairs. *Overview of Legislation*. Accessed: Jul. 30, 2018. [Online]. Available: https://www.homeaffairs.gov.au/about/national-security/telecommunications-interception-surveillance/overview-legislation

[67] *Telecommunications ACT 1997—SECT 313 Obligations of Carriers and Carriage Service Providers*. Accessed: Mar. 18, 2018. [Online]. Available: http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ta1997214/s313.html

[68] The Australian Communications and Media Authority. (2015). *Know Your Obligations Carriers and Carriage Service Providers, Including Internet and VoIP Service Providers*. Accessed: Jan. 5, 2018. [Online]. Available: http://creativecommons.org/licenses/by/3.0/au/

[69] Australian Department of Home Affairs. *Interception Capability Plans.* Accessed: Jul. 30, 2018. [Online]. Available: https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Interception-CapabilityPlans.aspx

[70] Legifrance. *Code des Postes et des Communications Électroniques—Article D98-7*. Accessed: Jan. 9, 2018. [Online]. Available: https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000025703459

[71] ICLG. (2017). *France Telecoms, Media & Amp; Internet 2018*. Accessed: Jan. 7, 2018. [Online]. Available: https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/france

[72] Legifrance. *Code des Postes et des Communications Électroniques—Article L32*. Accessed: Jan. 9, 2018. [Online]. Available: https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000024506026

[73] D. M. De La Justice, (Dec. 2016). *Bulletin Officiel Du Ministère De La Justice*. Accessed on: Jan. 9, 2018. [Online]. Available: http://www.textes.justice.gouv.fr/art_pix/JUSD1635582C.pdf

[74] Legifrance. *Code de Procédure Pénale—Article 100* Accessed: Jan. 9, 2018. [Online]. Available: https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006575246

[75] Bundesministerium der Justiz und für Verbraucherschutz. *German Government,* Âğ *110 TKG—Einzelnorm*. Accessed: Jan. 10, 2018. [Online]. Available: https://www.gesetze-im-internet.de/tkg_2004/__110.html

[76] German Parliament. (Jun. 22, 2004). *Telecommunications Act (TKG)*, Accessed: Mar. 19, 2018. [Online]. Available: https://rm.coe.int/16806af19e

[77] Bundesnetzagentur, German Government. *Technical Telecoms Regulation*. Accessed: Jan. 10, 2018. https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/TechnicalRegulation/TechnicalRegulation_node.html

[78] *Technical Guideline for the Implementation of Legal Measures for the Surveillance of Telecommunications and the Disclosure of Information*, 7th ed. Bonn, Germany, TR TKÜV, Federal Netw. Agency, Jun. 2017.

[79] UK Statute Law Database. *Section 12—Regulation of Investigatory Powers Act 2000*. Accessed: Jan. 10, 2018. [Online]. Available: https://www.legislation.gov.uk/ukpga/2000/23/section/12

[80] Queen's Printer of Acts of Parliament. *The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002*. Accessed: Jan. 11, 2018. [Online]. Available: https://www.legislation.gov.uk/uksi/2002/1931/contents/made

[81] Statute Law Database. *Section 2—Regulation of Investigatory UK Powers Act 2000*. Accessed: Jan. 11, 2018. [Online]. Available: http://www.legislation.gov.uk/ukpga/2000/23/section/2

[82] (2016). *UK Home Office, Interception of Communications—Code of Practice*. Accessed: Jan. 11, 2018. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf

[83] *United Kingdom—Telecoms, Media, and Internet 2018*, document 14377BC, 2018. Accessed: Jan. 11, 2018. [Online]. Available: https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/united-kingdom

[84] US Government. *National Domestic Communications Assistance Center, Communications Assistance for Law Enforcement Act, Section 101*. Accessed: Jan. 11, 2018. [Online]. Available: https://ndcac.fbi.gov/calea/thelaw/section101

[85] US Government. *National Domestic Communications Assistance Center, Communications Assistance for Law Enforcement Act, Section 103*. Accessed: Jan. 11, 2018. [Online]. Available: https://ndcac.fbi.gov/calea/thelaw/section103

[86] US Government. *National Domestic Communications Assistance Center, Communications Assistance for Law Enforcement Act, Section 102*. Accessed: Jan. 11, 2018. [Online]. Available: https://ndcac.fbi.gov/calea/thelaw/section102

[87] US Government. *Federal Communications Commission, Communications Assistance for Law Enforcement Act*. Accessed: Jan. 11, 2018. [Online]. Available: https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[88] The New York Times. *Apple Goes to Court, and F. B. I. Presses Congress to Settle iPhone Privacy Fight*. Accessed: Jan. 11, 2018. [Online]. Available: https://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html

[89] T. Spring. *Oct. 6, 2017. US Top Law Enforcement Calls Strong Encryption a 'Serious Problem'*. [Online]. Available: https://threatpost.com/us-top-law-enforcement-calls-strong-encryption-a-serious-problem/128302/

[90] (Jun. 13, 2017). *National Security Statement | Prime Minister of Australia*. Accessed: Jan. 17, 2018. [Online]. Available: https://www.pm.gov.au/media/national-security-statement

[91] A. Azfar, K.-K. R. Choo, and L. Liu, "A study of ten popular android mobile VoIP applications: Are the communications encrypted?" in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 4858–4867, Accessed: Jan. 22, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/6759199/

[92] C. Forrest. (Jun. 15, 2016). *WWDC 2016: Apple to Require HTTPS Encryption on all iOS Apps by 2017—TechRepublic*. Accessed: Jan. 22, 2018. https://www.techrepublic.com/article/wwdc-2016-apple-to-require-https-encryption-on-all-ios-apps-by-2017/

[93] W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek, "Balancing security and usability in encrypted email," *IEEE Internet Comput.*, vol. 21, no. 3, pp. 30–38, May 2017. Accessed: Jan. 22, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7927866/

[94] W. Amir. (Jan. 10, 2018). *Best Encrypted Email Services for 2018*. HackRead, Accessed: Jan. 22, 2018. [Online]. Available: https://www.hackread.com/best-encrypted-email-services-2018/

[95] P. Teufl, T. Zefferer, and C. Stromberger, *Mobile Device Encryption Systems*. Berlin, Germany: Springer, 2013, pp. 203–216. Accessed: Jan. 23, 2018. [Online]. Available: http://link.springer.com/10.1007/978-3-642-39218-4_16

[96] (Aug. 29, 2017). *Smartphone Growth Expected to Remain Positive as Shipments Forecast to Grow to 1.7 Billion in 2021, According to IDC*. Accessed: Jan. 23, 2018. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS43010517

[97] (May 2017). *IDC: Smartphone Vendor Market Share*. IDC. Accessed: Jan. 24, 2018. [Online]. Available: https://www.idc.com/promo/smartphone-market-share/vendor

[98] Gadgets. (Aug. 3, 2017). *World's 10 Biggest smartphone Companies | Gadgets Now*. [Online]. Available: https://www.gadgetsnow.com/slideshows/worlds-10-biggest-smartphone-companies/photolist/59889191.cms

[99] A. Prakash. (Jan. 6, 2018). *6 Open Source Mobile OS Alternatives To Android in 2018*. It's FOSS, Accessed: Jan. 24, 2018. [Online]. Available: https://itsfoss.com/open-source-alternatives-android/

[100] NIST. (Jul. 29, 1993). *NIST Proposes Voluntary Federal Standard for Key Escrow Encryption*. Accessed: Jan. 25, 2018. [Online]. Available: https://www.nist.gov/news-events/news/1993/07/nist-proposes-voluntary-federal-standard-key-escrow-encryption

[101] B.-J. Koops. (Jul. 1995). *Crypto Law Survey*. [Online]. Available: ftp://ftp.cerias.purdue.edu/pub/doc/cryptography/Crypto_Law_Survey/CryptoLawSurvey.html

[102] EFF. (Oct. 5, 1995). *The Government Doesn't Want Key Escrow*. Accessed: Jan. 25, 2018. [Online]. Available: https://w2.eff.org/Privacy/Key_escrow/?f=ellison_key_escrow.paper.txt

[103] (Apr. 13, 2016). *Intelligence Committee Leaders Release Discussion Draft of Encryption Bill—Press Releases—United States Senator for California*. Accessed: Jan. 28, 2018. [Online]. Available: https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=EA927EA1-E098-4E62-8E61-DF55CBAC1649

[104] D. Kravets. (Jan. 13, 2015). U.K. Prime Minister Wants Backdoors Into Messaging Apps or He'll Ban Them | Ars Technica. Ars Technica. Accessed: Jan. 29, 2018. [Online]. Available: https://arstechnica.com/tech-policy/2015/01/uk-prime-minister-wants-backdoors-into-messaging-apps-or-hell-ban-them/

[105] G. Greenwald, E. MacAskill, L. Poitras, S. Ackerman, and D. Rushe. (Jul. 12, 2013). Microsoft Handed the NSA Access to Encrypted Messages. The Guardian. Accessed: Jan. 29, 2018. [Online]. Available: https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[106] (Mar. 2017). *Challenging Government Hacking in Criminal Cases*. Accessed: Feb. 2, 2018. [Online]. Available: https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf

[107] A. Blankstein. (Feb. 16, 2016). *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone—NBC News*. Accessed: Jan. 15, 2018. [Online]. Available: https://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701

[108] *Skype Encryption Stumps German Police*. Accessed: Jan. 11, 2018. [Online]. Available: https://www.reuters.com/article/us-security-internet-germany/skype-encryption-stumps-german-police-idUSL21173920071122
[109] C. Burack. (Jan. 28, 2018). *German Federal Police Use Trojan Virus to Evade Phone Encryption | News | DW | 27.01.2018, DW*. Accessed: Feb. 5, 2018. [Online]. Available: http://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466
[110] Australian Security Intelligence organisation. *ASIO's Special Powers*. Accessed: Feb. 9, 2018. [Online]. Available: https://www.asio.gov.au/special-powers.html
[111] Commonwealth Consolidated Acts. *Australian Security Intelligence Organisation Act 1979—Sect 25A Computer Access Warrant*. Accessed: Feb. 9, 2018. [Online]. Available: http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/asioa1979472/s25a.html
[112] Commonwealth Consolidated Acts. *Crimes Act 1914—Sect 3LA: Person With Knowledge of a Computer or a Computer System to Assist Access Etc*. Accessed: Feb. 9, 2018. [Online]. Available: http://www.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ca191482/s3la.html
[113] D. Quick, B. Martini, K.-K. R. Choo, D. Quick, B. Martini, and K.-K. R. Choo, "Google drive," in *Cloud Storage Forensics*. Amsterdam, The Netherlands: Elsevier, 2014, pp. 95–126. Accessed: Feb. 9, 2018. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/B9780124199705000053
[114] Australian Government Federal Register of Legislation, Surveillance Devices Act 2004, no. 152, 2004. [Online]. Available: https://www.legislation.gov.au/Details/C2016C00103, Accessed on: Feb. 10, 2018
[115] Electronic Frontiers Australia. (Mar. 12, 2006). *EFA Submission re Telec (Interception) Amendment Bill 2006*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.efa.org.au/Publish/efasubm-slclc-tiabill-2006.html#47_31
[116] Commonwealth Consolidated Acts. *Telecommunications (Interception And Access) Act 1979—Sect 46A: Issue of Named Person Warrant*. Accessed: Feb. 10, 2018. [Online]. Available: http://www6.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/taaa1979410/s46a.html
[117] L. Tung. (Mar. 11, 2009). Security Vendors to Block Aust Police Hacks | ZDNet. ZDNet. Accessed: Feb. 10, 2018. [Online]. Available: http://www.zdnet.com/article/security-vendors-to-block-aust-police-hacks/
[118] Infosecurity Magazine. (Mar. 11, 2009). *IT Security Vendors and Australian Police Embroiled in Technology Spat*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.infosecurity-magazine.com/news/it-security-vendors-and-australian-police/
[119] Commonwealth Consolidated Acts. *Law Enforcement (Powers And Responsibilities) Act 2002—Sect 75B: Access to and Downloading of Data From Computers (Including Access to Computers Outside Premises the Subject of a Warrant)*. Accessed: Feb. 10, 2018. [Online]. Available: http://www6.austlii.edu.au/cgi-bin/viewdoc/au/legis/nsw/consol_act/leara2002451/s75b.html
[120] Legifrance. (2011). *LOI n° 2011-267 du 14 Mars 2011 d'Orientation et de Programmation Pour la Performance de la Sécurité Intérieure—Article 36*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=2B9F5F7747B6078C5B2755922C7E0771.tplgfr24s_1?idArticle=JORFARTI000023707417&cidTexte=JORFTEXT000023707312&dateTexte=29990101&categorieLien=id
[121] Legifrance. (2016). *LOI n° 2016–731 du 3 Juin 2016 Renforçant la Lutte Contre le Crime Organisé, le Terrorisme et Leur Financement, et Améliorant l'efficacité et Les Garanties de la Procédure Pénale—Article 5*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=2B9F5F7747B6078C5B2755922C7E0771.tplgfr24s_1?idArticle=JORFARTI000032627284&cidTexte=JORFTEXT000032627231&dateTexte=29990101&categorieLien=id
[122] G. Vaciago and D. S. Ramalho. *Online Searches and Online Surveillance: The Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings*. Accessed: Feb. 10, 2018. [Online]. Available: http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252
[123] German Federal Constitutional Court. (Feb. 27, 2008). *Decisions—Provisions in the North-Rhine Westphalia Constitution Protection Act on online searches and on the Surveillance of the Internet Null and Void*. Accessed: Feb. 10, 2018. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html
[124] S. Herpig and S. Heumann. (Apr. 13, 2017). Germany's Crypto Past and Hacking Future. LAWFARE. Accessed: Feb. 11, 2018. [Online]. Available: https://lawfareblog.com/germanys-crypto-past-and-hacking-future
[125] V. Beuth and K. Biermann. (Jun. 23, 2017). Staatstrojaner: Dein Trojanischer Freund und Helfer. Zeit, Accessed: Feb. 14, 2018. [Online]. Available: http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss
[126] F. Freiling, C. Safferling, and C. Rückert, "Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen," *Juristische Rundschau*, vol. 2018, no. 1, pp. 9–22, Nov. 2017. Accessed: Feb. 12, 2018. [Online]. Available: http://www.degruyter.com/view/j/juru.2018.2018.issue-1/juru-2017-0104/juru-2017-0104.xml
[127] F. Eder. (2009). Humanistische Union: Publikationen: Vorgänge: Online-Artikel: Online-Artikel Detail. Humanistische Union. Accessed: Feb. 16, 2018. [Online]. Available: http://www.humanistische-union.de/nc/publikationen/vorgaenge/online_artikel/online_artikel_detail/browse/19/back/nach-autoren/article/der-bundestrojaner-ein-notwendiges-uebel/
[128] *Bundesministerium der Justiz und für Verbraucherschutz, German Government, § 20k Verdeckter Eingriff in Informationstechnische Systeme—BKAG*. Accessed: Feb. 16, 2018. [Online]. Available: https://www.gesetze-im-internet.de/bkag_1997/__20k.html
[129] German Federal Constitutional Court. (Apr. 20, 2016). Decisions—Constitutional Complaints Against the Investigative Powers of the Federal Criminal Police Office for Fighting International Terrorism Partially Successful. Bundesverfassungsgericht. Accessed: Feb. 16, 2018. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/04/rs20160420_1bvr096609en.html
[130] MI5. *Equipment Interference*. Accessed: Feb. 16, 2018. [Online]. Available: https://www.mi5.gov.uk/equipment-interference
[131] M. Burgess. (May. 8, 2017). Investigatory Powers Bill: What is the Snoopers Charter and How Will it Affect You? WIRED. Accessed: Feb. 16, 2018. [Online]. Available: http://www.wired.co.uk/article/ip-bill-law-details-passed
[132] A. Travis. (Feb. 6, 2015). U.K. Government Issues First Definition of Computer Hacking by Spies | World News | The Guardian. The Guardian. Accessed: Feb. 17, 2018. [Online]. Available: https://www.theguardian.com/world/2015/feb/06/uk-government-definition-computer-hacking
[133] U.K. Home Office. (2016). *Equipment Interference: Code of Practice*. Accessed: Feb. 16, 2018. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf
[134] The Official Home of UK Legislation. (2016). *Part 5 Equipment Interference—Investigatory Powers Act 2016*. Accessed: Feb. 18, 2018. [Online]. Available: http://www.legislation.gov.uk/ukpga/2016/25/part/5
[135] UK Home Office. (2015). *Factsheet-Targeted Equipment Interference Investigatory Powers Bill*. Accessed: Feb. 18, 2018. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473740/Factsheet-Targeted_Equipment_Interference.pdf
[136] UK Home Office. (Feb. 2017). *DRAFT Equipment Interference Code of Practice*. Accessed: Feb. 18, 2018. [Online]. Available: http://www.gov.uk/government/collections/investigatory-powers-bill
[137] J. S. Granick, (Nov. 2, 2017). Challenging Government Hacking Whats Stake. ACLU. [Online]. Available: https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake
[138] J. J. Roberts. (Nov. 30, 2016). Rule 41 Grants New Hacking Powers to FBI|Fortune. Fortune. Accessed: Feb. 18, 2018. [Online]. Available: http://fortune.com/2016/11/30/rule-41/
[139] U.S. Department of Justice. (Jun. 20, 2016). *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*. Accessed: Feb. 18, 2018. [Online]. Available: https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches

[140] U.S.Department of Justice. (Nov. 28, 2016). *Additional Considerations Regarding the Proposed Amendments to the Federal Rules of Criminal Procedure*. Accessed: Feb. 18, 2018. [Online]. Available: https://www.justice.gov/archives/opa/blog/additional-considerations-regarding-proposed-amendments-federal-rules-criminal-procedure

[141] R. M. Thompson II. (Sep. 8, 2016.). Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure. Congressional Research Service. Accessed: Feb. 18, 2018. [Online]. Available: https://fas.org/sgp/crs/misc/R44547.pdf

[142] Legal Information Institute. *Rule 41. Search and Seizure|Federal Rules of Criminal Procedure*. Accessed: Feb. 18, 2018. [Online]. Available: https://www.law.cornell.edu/rules/frcrmp/rule_41

[143] K. Poulsen. (Jul. 18, 2007). FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats. WIRED. Accessed: Feb. 20, 2018. [Online]. Available: https://www.wired.com/2007/07/fbi-spyware/?currentPage=all

[144] D. Mccullagh. (Jan. 4, 2002). Judge OKs FBI Keyboard Sniffing. WIRED. Accessed: Feb. 20, 2018. [Online]. Available: https://www.wired.com/2002/01/judge-oks-fbi-keyboard-sniffing/

[145] T. Bridis. (Nov. 23, 2001). FBI is Building a 'Magic Lantern'. The Washington Post. Accessed: Feb. 20, 2018. [Online]. Available: https://www.washingtonpost.com/archive/politics/2001/11/23/fbi-is-building-a-magic-lantern/ca972123-83a8-46d8-b95c-c2edafda0fea/?utm_term=.1509218dea67

[146] B. Sullivan. (Nov. 20, 2001). FBI Software Cracks Encryption Wall—Technology & Science—Security. NBC News. Accessed: Feb. 20, 2018. [Online]. Available: http://www.nbcnews.com/id/3341694/ns/technology_and_science-security/t/fbi-software-cracks-encryption-wall/#.Wot3OLyWYs5

[147] K. Poulsen. (Aug. 5, 2014). Visit the Wrong Website, and the FBI Could End Up in Your Computer. WIRED. Accessed: Feb. 21, 2018. [Online]. Available: https://www.wired.com/2014/08/operation-torpedo/

[148] J. Valentino-DeVries and D. Yadron. (Aug. 2, 2013). FBI Taps Hacker Tactics to Spy on Suspects— Law-Enforcement Officials Expand Use of Tools Such as Spyware as People Under Investigation 'Go Dark. ProQuest. Accessed: Feb. 21, 2018. [Online]. Available: https://search.proquest.com/docview/1416642164/61187728977E4365PQ/1?accountid=14229

[149] C. Timberg and E. Nakashima. (Dec. 6, 2013). FBI's Search for 'Mo' Suspect Bomb Threats, Highlights use Malware for Surveillancet. The Washington Post. Accessed: Feb. 21, 2018. [Online]. Available: https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html?utm_term=.12c38fb8d073

[150] Z. Whittaker. (Mar. 6, 2017). Drops Playpen Child Porn Case to Prevent Release of Tor hackt. Justice Dept. Accessed: Feb. 21, 2018. [Online]. Available: http://www.zdnet.com/article/justice-dept-asks-to-drop-playpen-child-porn-case-to-prevent-releasing-tor-exploit/

[151] R. Gallagher. (Nov. 1, 2011). Governments Turn to Hacking Techniques for Surveillance of Citizens|Technology. The Guardian. Accessed: Feb. 21, 2018. [Online]. Available: https://www.theguardian.com/technology/2011/nov/01/governments-hacking-techniques-surveillance

[152] A. Hern. (Jul. 6, 2015). "Hacking Team Hacked: Firm Sold Spying Tools to Repressive Regimes, Documents Claim. The Guardian. Accessed: Feb. 21, 2018. [Online]. Available: https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim

[153] (2015). *WikiLeaks—The Hackingteam Archives*. Accessed: Feb. 21, 2018. [Online]. Available: https://wikileaks.org/hackingteam/emails/

[154] P. Paganini. (Jul. 21, 2015). *When Hackers Become Targets*. Infosec Inst. Accessed: Feb. 21, 2018. [Online]. Available: http://resources.infosecinstitute.com/the-hacking-team-hack-when-hackers-have-become-the-target/#gref

[155] M. Marquis-Boire, J. Scott-Railton, C. Guarnieri, and A. Kleemola. (Jun. 24, 2014). Hacking Team's Tradecraft and Android Implant. The Citizen Lab. Accessed: Feb. 21, 2018. [Online]. Available: https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/

[156] B. Knight. (Sep. 5, 2012). UK Malware Used Against Bahraini Activists|World|Breakings News and Perspectives From Around the Globe. Deutsche Welle. Accessed: Feb. 21, 2018. [Online]. Available: http://www.dw.com/en/uk-malware-used-against-bahraini-activists/a-16219440

[157] B. Knight. (Sep. 19, 2012). German Spyware Business Supports Dictators|World|Breakings News and Perspectives From Around the Globe|. Deutsche Welle. Accessed: Feb. 21, 2018. [Online]. Available: http://www.dw.com/en/german-spyware-business-supports-dictators/a-16249165

[158] V. Blue. (Aug. 6, 2014). *Top gov't Spyware Company Hacked; Gamma's FinFisher Leaked*. Accessed: Feb. 21, 2018. [Online]. Available: http://www.zdnet.com/article/top-govt-spyware-company-hacked-gammas-finfisher-leaked/

[159] (Dec. 1, 2011). *WikiLeaks—The Spy Files*. WikiLeaks. Accessed: Feb. 21, 2018. [Online]. Available: https://wikileaks.org/spyfiles/list/releasedate/2011-12-08.html

[160] (Sep. 15, 2014). *WikiLeaks—SpyFiles 4*. WikiLeaks. Accessed: Feb. 21, 2018. [Online]. Available: https://wikileaks.org/spyfiles4/

[161] A. Meister. (Aug. 6, 2014.). Gamma FinFisher Hacked: 40 GB of Internal Documents and Source Code of Government Malware Published. Netzpolitik.org. Accessed: Feb. 21, 2018. [Online]. Available: https://netzpolitik.org/2014/gamma-finfisher-hacked-40-gb-of-internal-documents-and-source-code-of-government-malware-published/

[162] (Dec. 1, 2011). *Finfisher: Governmental IT Intrusion and Remote Monitoring Solutions—Product Portfolio WikiLeaks—The Spy Files*. Accessed: Feb. 22, 2018. [Online]. Available: https://wikileaks.org/spyfiles/docs/gamma/299_finfisher-governmental-it-intrusion-and-remote-monitoring.html

[163] J. Valentino-DeVries. (Nov. 21, 2011). Surveillance Company Says It Sent Fake iTunes, Flash Updates. The Wall Street J. Accessed: Feb. 22, 2018. [Online]. Available: https://blogs.wsj.com/digits/2011/11/21/surveillance-company-says-it-sent-fake-itunes-flash-updates-documents-show/

[164] F. Kafka. (Sep. 21, 2017).*ESET Finds Internet Providers may be Involved in Latest FinFisher Surveillance Campaigns*. ESET. Accessed: Feb. 22, 2018. [Online]. Available: https://www.eset.com/us/about/newsroom/press-releases-list/press-releases/eset-finds-internet-providers-may-be-involved-in-latest-finfisher-surveillance-campaigns/

[165] (Mar. 7, 2017). *Vault 7: CIA Hacking Tools Revealed*. WikiLeaks. Accessed: Feb. 22, 2018. [Online]. Available: https://wikileaks.org/ciav7p1/

[166] (2017). *Weeping Angel—Extending—User Guide*. WikiLeaks. Accessed: Feb. 23, 2018. [Online]. Available: https://wikileaks.org/vault7/document/EXTENDING_User_Guide/#pfe

[167] WikiLeaks. (2017). *DarkSeaSkies v1.0–User Manual*. Accessed: Feb. 23, 2018. [Online]. Available: https://wikileaks.org/vault7/document/DarkSeaSkies_1_0_User_Manual

[168] J. Grover, "Android forensics: Automated data collection and reporting from a mobile device," *Digit. Invest.*, vol. 10, pp. S12–S20, Aug. 2013.

[169] A. Hernandez. (Nov.29, 2017). Support for latest IOS and android mobile devices. Blackbag Technologies. Accessed: Jun. 13, 2018. [Online]. Available: https://www.blackbagtech.com/blog/2017/11/29/mobilyze-2017-r1-1-now-available

[170] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, "Current and future trends in mobile device forensics: A survey," *ACM Comput. Surv.*, vol. 51, no. 3, Jul. 2018, Art. no. 46. Accessed: Jun. 15, 2018. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3212709.3177847

[171] M. Oltrogge, Y. Acar, S. Dechand, M. Smith, and S. Fahl, "To pin or not to pin—Helping app developers bullet proof their TLS connections," in *Proc. 24th USENIX Conf. Secur. Symp.*, 2015, pp. 239–254. Accessed: Jun. 22, 2018. [Online]. Available: https://dl.acm.org/citation.cfm?id=2831159

[172] A. Razaghpanah, A. A. Niaki, N. Vallina-Rodriguez, S. Sundaresan, J. Amann, and P. Gill, "Studying TLS usage in Android apps," in *Proc. 13th Int. Conf. Emerg. Netw. Exp. Technol. (CoNEXT)*, 2017, pp. 350–362. Accessed: Jun. 21, 2018. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3143361.3143400

[173] F. Sierra and A. Ramirez, "Defending your Android app," in *Proc. 4th Annu. ACM Conf. Res. Inf. Technol. (RIIT)*, 2015, pp. 29–34. Accessed: Jun. 21, 2018. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2808062.2808067

[174] T. Espiner. (Jul. 2011). Vodafone femtocell hack lets intruders listen to calls. ZDNet. Accessed: Jun. 24, 2018. [Online]. Available: https://www.zdnet.com/article/vodafone-femtocell-hack-lets-intruders-listen-to-calls

[175] N. Golde, K. Redon, and R. Borgaonkar, "Weaponizing femtocells: The effect of rogue devices on mobile telecommunication," in *Proc. 19th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2012, pp. 1–16. Accessed: Jun. 24, 2018. [Online]. Available: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/P03_4.pdf

[176] T. Ritter. Femtocell presentation slides, videos and app. NCC Group. Accessed: Aug. 19, 2013. [Online]. Available: https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2013/august/femtocell-presentation-slides-videos-and-app

[177] E. Gelenbe *et al.*, "Security for smart mobile networks: The NEMESYS approach," in *Proc. Int. Conf. Privacy Secur. Mobile Syst. (PRISMS)*, Jun. 2013, pp. 1–8. Accessed: Jun. 24, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/6927181

[178] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2016, pp. 1118–1130. Accessed: Jun. 25, 2018. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2976749.2978393

[179] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016. Accessed: Jun. 26, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7547270/

[180] L. He, Z. Yan, and M. Atiquzzaman, "LTE/LTE-A network security data collection and analysis for security measurement: A survey," *IEEE Access*, vol. 6, pp. 4220–4242, 2018. Accessed: Jun. 24, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/8255622

[181] Tor Project. *Tor Onion Service—Configuring Onion Services for Tor*. Accessed: Jun. 20, 2018. [Online]. Available: https://www.torproject.org/docs/tor-onion-service.html.en

[182] J. Watson. (Feb. 7, 2017). How to set up a hidden tor service or .Onion Website. Comparitech. Accessed: Jun. 20, 2018. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/how-to-set-up-a-tor-hidden-service

[183] HackingTeam. *RCS 9.6 The Hacking Suite for Governmental Interception–Technician Manual*. Accessed: Mar. 2015. [Online]. Available: https://wikileaks.org/hackingteam/emails/fileid/1062721/494372

[184] Chaos Computer Club. (Oct. 8, 2011). *CCC | Chaos Computer Club Analyzes Government Malware*. Accessed: Feb. 24, 2018. [Online]. Available: https://ccc.de/en/updates/2011/staatstrojaner

[185] M. Marquis-Boire, B. Marzcak, C. Guarnieri, and J. Scott-Railton. (Mar. 13, 2013). You only click twice: FinFisher's global proliferation. Citizen Lab. Accessed: Feb. 24, 2018. [Online]. Available: https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2

[186] Trend Micro. (Aug. 20, 2015). *7 Things You Need To Know About the Hacking Team's Leaked Mobile Malware Suite*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-things-about-hacking-team-leaked-mobile-malware-suite

[187] R. Joyce. (Nov. 15, 2017). Improving and making the vulnerability equities process transparent is the right thing to do. White House. Accessed: Feb. 24, 2018. [Online]. Available: https://www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing

[188] National Cryptologic Museum Foundation. (Nov. 25, 2017). *Cryptologic Bytes Archives—Vulnerabilities in the Spotlight—Vulnerabilities Equity Process (VEP)*. Accessed: Feb. 24, 2018. [Online]. Available: https://cryptologicfoundation.org/learn/educate/bytes/cryptologic_bytes_archives1.html/article/2017/11/25/vulnerabilities-in-the-spotlight-vulnerabilities-equity-process-vep

[189] Microsoft. (Feb. 14, 2017). *The Need for a Digital Geneva Convention–Microsoft on the Issues*. Accessed: Mar. 08, 2018. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001gnysbhjsod01z7q11hvz0xg2d

[190] National Institute of Standards and Technology. *NIST Computer Forensic Tool Testing Program*. Accessed: Feb. 25, 2018. [Online]. Available: https://www.cftt.nist.gov

[191] Department of Homeland Security. *NIST CFTT Reports | Homeland Security*. Accessed: Feb. 24, 2018. [Online]. Available: https://www.dhs.gov/science-and-technology/nist-cftt-reports

[192] *Information Technology–Security Techniques–Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*, International Organization for Standardization, Standard ISO/IEC 27037:2012, 2012. Accessed: Feb. 24, 2018. [Online]. Available: https://www.iso.org/standard/44381.html

[193] T. Spring. (Apr. 25, 2016). Android ransomware attacks using towelroot, hacking team exploits. Threatpost. Accessed: Jul. 09, 2018. [Online]. Available: https://threatpost.com/android-ransomware-attacks-using-towelroot-hacking-team-exploits/117655

CHEN-YU LI received the B.S.E.E. degree from Chung Yuan Christian University, Taoyuan, Taiwan, in 2005, and the M.S. degree in electronic and computer engineering from the National Taiwan University of Science and Technology in 2007. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Graduate Institute of Communication Engineering, National Taiwan University. His research interests include optical and wireless communication systems, computer networks, digital forensics, anonymity and privacy, lawful interception, and network security.

CHIEN-CHENG HUANG received the M.S. degree in information management from the National Chiao Tung University in 2008 and the Ph.D. degree in information management from National Taiwan University in 2014. He served as an Adjunct Assistant Professor with Central Police University. He has over 10 years of experience in information technology industry. His current research interests include data mining, artificial intelligence, cyber/ICT/IoT/IIoT security, and cyber/network forensics.

FEIPEI LAI (SM'94) received the B.S.E.E. degree from National Taiwan University in 1980, and the M.S. and Ph.D. degrees in computer science from the University of Illinois at Urbana–Champaign in 1984 and 1987, respectively. He was a Vice Superintendent with the National Taiwan University Hospital, the Chairman of the Taiwan Network Information Center, and a Visiting Professor with the Department of Computer Science and Engineering, University of Minnesota, Minneapolis, MN, USA. He was also a Guest Professor with the University of Dortmund, Germany, and a Visiting Senior Computer System Engineer with the Center for Supercomputing Research and Development, University of Illinois at Urbana–Champaign. He is currently a Professor with the Department of Computer Science and Information Engineering, Graduate Institute of Biomedical Electronics and Bioinformatics, and the Department of Electrical Engineering, National Taiwan University. He currently holds 10 Taiwan patents and four U.S. patents.

SAN-LIANG LEE (SM'07) received the Ph.D. degree in electrical and computer engineering from the University of California at Santa Barbara in 1995. He joined the Faculty of the Department of Electronic Engineering, National Taiwan University of Science and Technology (NTUST) in 1988 and became a Full Professor in 2002. He served as the Vice President of the university from 2011 to 2014. He was the Chairman of the Department from 2005 to 2008. He served as the Dean of the Academic Affairs Office, NTUST, from 2008 to 2010. He was the Director of the Program Office for the National Innovative Education Program on Image Display Technology, sponsored by the Ministry of Education, Taiwan, from 2005 to 2009. He was a Visiting Scientist with the Research Laboratory of Electronics, Massachusetts Institute of Technology, by taking a sabbatical leave from NTUST from 2010 to 2011. He has published over 200 referred papers in international journals and conferences and holds 30 patents. His research interests include semiconductor optoelectronic components, photonic integrated circuits, nanophotonics, and optical networking technologies. He served as an Electronic Section Editor of the SCI indexed *Journal of the Chinese Institute of Engineers* from 2007 to 2012.

JINGSHOWN WU (M'78–SM'99–F'05–LF'09) received the B.S. and M.S. degrees in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1970 and 1972, respectively, and the Ph.D. degree from Cornell University, Ithaca, NY, USA, in1978. He joined Bell Laboratories in 1978, where he was involved in digital network standards and performance and optical fiber communication systems. In 1984, he joined the Department of Electrical Engineering, National Taiwan University, as a Professor and was the Chairman of the Department from 1987 to 1989.

He was also the Director of the Communication Research Center, College of Engineering of the university, from 1992 to 1995. From 1995 to 1998, he was the Director of the Division of Engineering and Applied Science, National Science Council, China, on leave from the university. From 1999 to 2002, he was the Chairman of the Commission on Research and Development and the Director of the Center for Sponsor Programs, National Taiwan University. He was the Vice President of the university from 2002 to 2005. He was the Chairman of the Institute for Information Industry from 2006 to 2007. He has published over 160 journal and conference papers and holds 16 patents. He is interested in optical fiber communications, computer communications, and communication systems. He received the Distinguished Research Awards and a Distinguished Research Fellow from the National Science Council, China, from 1991 to 1996 and from 1996 to 2002. He was a recipient of the Outstanding Engineering Professor Award from the Chinese Institute of Engineers in 1996 and the Engineer Metal Award from the Institute of Chinese Electrical Engineers in 2006, and the Award from CIE/USA in 2009.

He is a life member of the Chinese Institute of Engineers, the Optical Society of China, and the Institute of Chinese Electrical Engineers. He served as the Vice Chairman from 1997 to 1998 and the Chairman from 1998 to 2000 of the IEEE Taipei Chapter. He is also a member of the IEEE Communications Society Award Committee from 2006 to 2008, the IEEE Communications Society Fellow Evaluation Committee 2008, and the IEEE Fellow Committee from 2009 to 2012.