November 2018 · Dr. Sven Herpig

A Framework for Government Hacking in Criminal Investigations

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Table of Contents

1. Introduction

Since the first *crypto war*[1] of the 1990s, governments have occupied themselves with the perceived and real challenges for law enforcement which arise from encryption technologies[2]. While encryption enables secure communications that are vital for society, the economy, and the government itself[3], it can also be used by criminals to easily hide their communication and certain data from law enforcement. The FBI refers to the so-called "going dark" challenge as "a real and growing gap between law enforcement's legal authority to access digital information and its technical ability to do so"[4] -- even though law enforcement seems to not have assessed this issue thoroughly[5]. Over the years, there have been numerous proposals[6] to tackle this purported issue, such as government-mandated backdoors, a weakening of encryption standards,[7] and direct access[8]. This debate has recently been reinvigorated by the simultaneous publication of reports by the National Academy of Sciences - Engineering - Medicine[9] (NAP) and the EastWest Institute (EWI)[10]. The NAP report laid out a broad range of questions by which any proposed encryption policy should be tested; the EWI focused instead on the pros and cons of "lawful hacking" and design mandates.

While there is a great variety of perspectives and opinions on the alleged "going dark" problem, most experts still agree on the fundamental point

1 Danielle Kehl, Andi Wilson and Kevin Bankston, Doomed to Repeat History? Lessons learned from the Crypto Wars of the 1990s

2 Government hacking is not merely a law enforcement response to the existence and widespread use of encryption technology but to digitalization in general, see for example US v. Gorshkov

3 Danielle Kehl, Andi Wilson and Kevin Bankston, Doomed to Repeat History? Lessons learned from the Crypto Wars of the 1990s

4 Christopher A. Wray, Statement of Christopher A. Wray Director Federal Bureau of Investigation, Department of Justice

5 Ari Schwartz, In the dark about 'going dark'
Devlin Barrett, FBI repeatedly overstated encryption threat figures to Congress, public

6 Sayako Quinlan and Andi Wilson, A Brief History of Law Enforcement Hacking in the United States

7 Larry Greenemeier,NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard

8 National Academies of Sciences - Engineering - Medicine, Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext

9 National Academies of Sciences - Engineering - Medicine, Decrypting the Encryption Debate: A Framework for Decision Makers

10 Andreas Kuehn and Bruce McConnell, Encryption Policy in Democratic Regimes - Finding Convergent Paths and Balanced Solutions

that strong encryption is the basis for secure digital communications, and weakening encryption, or requiring providers of encrypted products or services to redesign their offerings in order to facilitate government access[11], weakens security. A leaked 2009 US National Security Council document described encryption as the best defense to protect data, and warned that government and private sector systems were subject to attacks because of cryptography's slow deployment[12]. Several countries, among them Germany[13] and the United States[14], have taken to enabling law enforcement to conduct investigations via hacking tools -- referred to as "government hacking," "lawful hacking," or "equipment interference" -- in order to access encrypted communications, pierce through anonymity-enabling technologies such as The Onion Router (TOR)[15], or possibly even to avoid more tedious legal procedures to access information (e.g. through Mutual Legal Assistance Treaties – MLATs).

Governments view hacking as a partial alternative to regulating encryption. It is sometimes presented as a compromise between taking no action and mandating encryption backdoors. While government hacking might indeed be a partial solution to the purported going dark challenge, it is no panacea. It still has serious shortcomings that pose serious threats to human rights, privacy[16], IT security, and ultimately national security[17]. Stockpiling certain vulnerabilities, for example, might make government hacking more effective, but at the same time it may keep systems vulnerable which can be exploited by criminals and state-backed attackers. When it comes to privacy concerns, government hacking can be extremely invasive and have unanticipated consequences, resulting from the vast amounts of multimedia data, communications, connected (Internet-of-Things) devices and sensors, all of

11 Transatlantic Cyber Forum, Initial Take-Away: Encryption Policy and "Government Hacking"

12 James Ball, Secret US cybersecurity report: encryption vital to protect private data

13 Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers and Cathleen Berger, Is Germany (involuntarily) setting a global digital agenda?

14 Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

15 Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers

16 Report of the U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40, para. 62, 17 Apr. 2013

17 Sven Herpig, Government Hacking - Global Challenges

which can potentially be accessed by law enforcement agencies during a government hacking operation.

Government hacking raises the following risks:

- Creating a government hacking industry and driving vulnerability markets;
- Potential loss of exclusive control by government over its hacking tools[18];
- Subverting (IT-)security, e.g. compromising communication infrastructure;
- Decreasing user trust, e.g. in IT-companies;
- Broadly targeting a large amount of highly private information;
- Hacking innocent users as "collateral damage" of hacking campaigns;
- Through chilling effects decreasing freedom of expression;
- Potential loss of integrity of electronic evidence;
- Extraterritorial implications;
- Liability concerns.

This paper suggests a minimum standard for how governments should behave when hacking[19]. These underlying requirements attempt to address investigatory needs, human rights, privacy rights, IT security, and national security[20]. These requirements are categorized into more general "structural" recommendations to govern a state's government hacking program, and "operational" recommendations to govern the conduct of government hacking. The minimum standard for government hacking operations suggested in this paper through operational and structural requirements does not solve

18 Check Point IPS Research Team, BROKERS IN THE SHADOWS: Analyzing vulnerabilities and attacks spawned by the leaked NSA hacking tools

19 Parts of those minimum requirements could technically also be applied on the EU level following Article 82(2) TFEU, European Parliament Directorate-General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices STUDY

20 This paper is based on the principle that weakening device security - e.g. through mandating backdoors or stockpiling vulnerabilities for government hacking - is not only affecting users' privacy and IT security in general but ultimately national security at-large. Additionally, due to the serious invasiveness of government hacking, this framework was designed giving premium to human rights principles such as proportionality and necessity. It is however unclear, if - due to its invasive nature - government hacking will ever be able to meet those requirements.
Privacy International, Hacking Safeguards and Legal Commentary

all above mentioned challenges but aims to substantially mitigate their potential negative impact.

Structural requirements form the pillars of a basic framework for government hacking:

1. Establish a legal framework for government hacking.
2. Foster research on encryption and government hacking workarounds.
3. Set up a capacity building program.
4. Implement guidelines for handling digital evidence.
5. Establish an interagency dialogue.
6. Limit government hacking to serious crimes.
7. Implement transparency reporting.
8. Define binding requirements for vendors of government hacking tools.
9. Establish a national vulnerability assessment and management process.

Operational requirements define how government hacking should be conducted:

- Requirements for a predictable framework such as handling of privileged communication and compelling third-party assistance.
- Requirements to maintain a high level of security and privacy, such as securing government hacking tools and vulnerabilities with state-of-the-art measures.
- Requirements for prior judicial oversight, such as required warrants.

2. Defining "Government Hacking"

While the British prefer to speak of "equipment interference," "government hacking" and "lawful hacking" are the more widely used terms for the activity being discussed in this paper. In countries such as the United States, there is no distinct legal framework for this activity[21], casting doubts on the lawfulness and legal boundaries of government hacking operations. This paper works with the following definition of government hacking: "interfering with the integrity of software – including online services – or hardware to access data in transit, data at rest, and sensors to manipulate a target's device by law enforcement for the purpose of criminal investigations". The practice includes the deployment of malicious software (malware), which is either developed in-house or procured from vendors or contractors. Such malware can be installed on a target's device either remotely or through gaining physical access to the device itself. A remote government hacking operation can be conducted through cooperation with technology companies and Internet

21 Jonathan Mayer, Government Hacking

Service Providers[22], through waterholing[23], and through other techniques also used by criminals, foreign militaries, and intelligence agencies.

While government hacking has mainly been discussed within the context of the encryption debate (i.e. "going dark" in law enforcement access to data), government hacking can also be applied to devices that do not use encryption but are, for example, protected by other security mechanisms (e.g. access to a password-protected operating system). Government hacking has also been identified by governments as an option to respond to cyber crime under the notion of "active cyber defense/ hack backs". This is the idea that law enforcement should be permitted to respond to cyber-crime by disabling or destroying the machines that were the source of the attack. Government hacking is however not primarily about countering cyber crime, nor is it particularly well-suited[24] to do so. Instead, it is most useful for law enforcement when investigators need access to digital devices that supposedly hold criminal evidence or to track or identify the perpetrator of a crime. According to the definition introduced here, military and intelligence cyber operations without law enforcement purposes are explicitly *not* government hacking for the purposes of this paper.

22 Filip Kafka, New FinFisher surveillance campaigns: Internet providers involved?

23 Operation Pacifier conducted by the FBI is a prime example of a law enforcement waterholing attack. Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

24 Cyber crime, for example the rampant threat of ransomware, is best responded to by increasing IT security and resilience.

3. Structural Requirements

3.1 Establish a legal framework for government hacking

A distinct framework for government hacking needs to be codified in law. This is due to the privacy invasiveness and security risks that are inherent to government hacking, and because it is vital to clarify the rules applying to everyone involved[25]. International human rights law, for example, states that a clear framework is the first necessary requirement to legitimate the government's interference with privacy[26]. The Office of the United Nations High Commissioner for Human Rights stated in 2018 that "[l]aws should be established or amended to specify clearly that restrictions on encryption and anonymity tools, including government hacking measures, are permitted only in exceptional circumstances; i.e. when they satisfy the requirements of legality, necessity and proportionality, and legitimacy of objective. Government authorities should refrain from relying on generic or antiquated laws to justify restrictions on encryption and anonymity tools that do not satisfy these criteria."[27]

Further, there needs to be a central, legal framework for government hacking that is distinct from existing criminal law and proscribed to modern technologies due to the complexity and distinct nature of information technology[28]. Only then can law enforcement be certain that their hacking activities are within the law and that citizens are appropriately protected from the state. Deriving investigatory powers from non-cyber specific laws should be the exception and not the norm. A legal framework for government hacking needs to incorporate the structural and operational requirements presented in this paper.

Whereas legal safeguards have not been implemented in the US with regards to government hacking, they have been established for government surveil-

25 Susan Hennessey, The Elephant in the Room: Addressing Child Exploitation and Going Dark

26 United Nations, The Right to Privacy in the Digital Age - Report of the Office of the United Nations High Commissioner for Human Rights

27 Office of the United Nations High Commissioner for Human Rights, Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Encryption and Anonymity follow-up report, Research Paper 1/2018

28 Jennifer Granick, SCOTUS & Cell Phone Searches: Digital is Different
Jonathan Mayer, Government Hacking

lance measures in the Wiretap Act ("Title III")[29]. Similar safeguards for government hacking should therefore follow. Germany has established a legal framework for government hacking[30], which has just recently been updated in 2017[31].

3.2 Foster research on encryption and government hacking workarounds

Even law enforcement representatives admit that sometimes there are workarounds that allow law enforcement agencies to gather sufficient evidence without weakening encryption or conducting government hacking operations[32]. While those alternatives to collect (digital) evidence might be more time consuming and not as easy to scale, it is worthwhile for governments to explore those workarounds to government hacking. Some research has already been conducted in that area[33]. They might in some instances be less invasive, or even faster to implement[34]. A starting point for governments would be to increase transparency by reporting how often workarounds lead to acquiring the sought-after evidence. A tactic could be identifying the troves of information that are a byproduct of digitization[35], which are already

29 Office of Justice Programs, Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)

30 Inter alia §100 Code of Criminal Procedure

31 Deutscher Bundestag, Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens
TCF Policy Debate, Intensification of targeted surveillance of suspects via so called 'state trojan' software

32 Christopher A. Wray, Statement of Christopher A. Wray Director Federal Bureau of Investigation, Department of Justice

33 Orin S. Kerr and Bruce Schneier, Encryption Workarounds
Riana Pfefferkorn, The Risks of "Responsible Encryption"
European Digital Rights, Encryption Workarounds
National Academies of Sciences - Engineering - Medicine, Decrypting the Encryption Debate: A Framework for Decision Makers
Andrew Keane Woods, Encryption Substitutes
William A. Carter and Jennifer C. Daskal, Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge

34 In the case United States of America v. David Conerly obtaining the password to unlock the mobile device of the alleged perpetrator through monitoring the telephone calls he made from jail was faster than going through the channels to have specialized FBI units unlock the device.
United States of America v. David Conerly, Order Denying Defendant's Motion to Suppress, Case No. 17-cr-00578-JSW-1

35 National Academies of Sciences - Engineering - Medicine, Decrypting the Encryption Debate: A Framework for Decision Makers
accessnow, Encryption in the U.S.: Crypto Colloquium Outcomes Report

legally and technically accessible to law enforcement. With a demonstration that legal standards, including privacy protections, are satisfied, sources for this range from data and backups on cloud-type servers (especially email inboxes), to metadata[36], telemetry, Internet-of-Things sensors, and biometric authentication features. There is also the option for law enforcement agencies to conduct so called "old school" surveillance for obtaining the passcode to a device[37]. Therefore, it is uncertain whether law enforcement actually has a legitimate point in demanding legal and technical government hacking capabilities, or whether this is just the easiest way to gain access. Thus, governments should conduct research that identifies and describes all possible sources and methods to access digital evidence without the use of government hacking or weakening of encryption[38], as well as the real extent of the "going dark" challenge[39]. Doing so might be challenging and resource-intensive, but without this effort, making a well-reasoned public policy decision is nearly impossible. It should also analyze the gap regarding operational value to law enforcement of digital evidence obtained with and without government hacking.

3.3 Set up a capacity building program

Government hacking involves complex technical issues and leads to privacy invasion and security risks[40]. Understanding government hacking and its implications is therefore a challenging task and requires special expertise. From a rule of law perspective, this expertise should not only be concentrated in law enforcement. Otherwise, no serious oversight and check from judiciary is possible. Capacity building is especially important as it pertains to the legality of government hacking. Therefore, training on how government hacking works, as well as on its privacy and security implications, should be offered to everyone in the judiciary working on government hacking and its warrant process. Additionally, technological experts should serve as court personnel as a resource for judges[41]. Everyone dealing with government hacking needs

36 Woods notes that metadata "is often as valuable or more so for law enforcement than content data". Andrew Keane Woods, Encryption Substitutes

37 Matthias Schulze, Verschlüsselung in Gefahr

38 A successful example that combines several traditional investigatory methods where no government hacking was required is the takedown of a darknet drug portal known as the Silk Road. Andy Greenberg, Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht

39 Susan Hennessey, Lawful hacking and the case for a strategic approach to "Going Dark"

40 Sven Herpig, Government Hacking - Global Challenges

41 US FISA Court Amicus might serve as a pointer. Ben Cook, The New FISA Court Amicus Should Be Able to Ignore its Congressionally Imposed Duty

to have access to workplace training that fosters a clear understanding of the issues involved, which might be limited in certain areas by classification. This includes anyone with a legal, political, or technical background. This can range from the integrity of the digital chain of evidence, digital signing, and how the security of devices in question are relevant to legal proceedings.

3.4 Implement guidelines for handling digital evidence

Analogous to the handling of non-digital evidence, governments need to design and implement guidelines for handling digital evidence. From the point that digital evidence is secured from a hacked device, it needs to be transferred, stored, and presented in a tamper-proof chain of custody (e.g. via digital signing of data and encrypted file transfers). Harming the integrity of digital evidence might be easier compared to non-digital evidence, as assessing a device already represents integrity loss, and therefore needs extra precautions. Such a precaution could be to, wherever possible, mirror the device and do forensics only on the copy and leave the original unaltered. The guidelines should be independently reviewed by IT security researchers, making sure that the protection mechanisms for the handling of digital evidence are state-of-the-art. The FBI for example has such a guideline[42]. It covers a wide range of issues, from maintenance of the chain of custody, to storage and shipping guidelines, and even to a multi-tiered approach for handling digital evidence for different purposes (content review, advanced technical analysis, etc.).

3.5 Establish an interagency dialogue

A government hacking operation can have possible ramifications far beyond the implementing agency. For example when the person behind the device is only known after it has been successfully compromised[43], someone who has special legal protection (journalist, diplomat, member of parliament) or is outside the scope of the warrant (foreigner living abroad for a purely domestic warrant) might be hacked. Therefore, it is prudent to establish a workflow that allows for an ad-hoc interagency dialogue. So far, empirical evidence suggests that domestically-focused law enforcement hacking operations that compromised devices around the world have not sparked international

42 U.S. Federal Bureau of Investigations, Digital Evidence Policy Guide

43 This was the case for example during the Operation Pacifier. It was designed in a way that everyone accessing a certain part of the compromised child porn portal was automatically infected by the FBI with a network investigative technique (NIT). Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

controversies[44]. However, it seems useful to involve the Ministry of Foreign Affairs in such a workflow to limit international spillover effects. Complaints from states who discover that another state hacked devices in their country cannot be ruled out. Similarly, informing other law enforcement and security agencies might yield increased operational value and a more efficient allocation of resources.

Additionally, a centralized interagency dialogue might be useful to increase efficiency of information sharing between the different levels of law enforcement. They could share best practices on what evidence exists outside of government hacking, knowledge about government hacking operations and available tools, as well as possibly even access to government hacking soft- and hardware. The latter is being organized in Germany through its Central Authority for Information Technology in the Security Sphere[45] (*Zentrale Stelle für Informationstechnik im Sicherheitsbereich*), which was founded in 2017.

3.6 Limit government hacking to "serious crimes"

Government hacking has serious ramifications for IT security and privacy; its deployment must be limited by applying strong safeguards for investigations and limit them to *serious crimes*. Non-serious crimes must not be the predicate for the use of government hacking. A recommendation made by Susan Hennessey, among others, lays out the potential benefits of this restriction, arguing that "limiting lawful hacking to serious cases ensures appropriate allocation of research and development resources, better protects tools, and facilitates coordinated prosecution strategies".[46]

Current applications of government hacking include a wide range of crimes such as tax evasion[47] and loan shark activities[48]. Several countries define a

44 Orin S. Kerr and Sean D. Murphy, Government Hacking to Light the Dark Web
Joseph Cox, The FBI Blindly Hacked Computers in Russia, China, and Iran

45 Zentrale Stelle für Informationstechnik im Sicherheitsbereich
TCF Policy Debate, Official Announcement about the Central Authority for Information Technology in the Security Domain

46 Susan Hennessey, Lawful hacking and the case for a strategic approach to "Going Dark"

47 German Ministry of Justice and Consumer Protection, The German Code of Criminal Procedure §100a

48 Jonathan Mayer, Government Hacking

list of serious crimes in which case government hacking is applicable, inter alia based on the maximum custodial sentence of the respective crime[49].

Which standard/model is applied for defining serious crimes is up to the respective government. It should however be codified as law and the application of government hacking limited to the crimes mentioned.

3.7 Implement transparency reporting

Publicly available data enables public debate and research. This includes independent review of current (legal) government hacking practices by stakeholders outside the government. Based on this publicly available information, trade-offs among law enforcement capabilities, IT-security drawbacks, and privacy invasiveness could be assessed. This would lead to a better informed policy-making process. Therefore, government hacking activities by law enforcement agencies should be published annually in a transparency report[50]. At a bare minimum it must include the number of government hacking operations that have been conducted, the suspected crime, how many subjects with special protection were targeted, the percentage of targets informed, and what percentage of warrants were denied by the judiciary.

3.8 Define binding requirements for vendors of government hacking tools

Hacking tools, vulnerabilities, and services for law enforcement purposes must only be acquired from third parties that are transparently vetted and that do not conduct any business with governments or other entities that have been reported to conduct unlawful government hacking or violate human rights. A due diligence audit needs to be conducted annually to avoid indirectly financing human rights abuses. A basis for this audit could be annual human rights reports from official and independent human rights bodies, including: Amnesty International, Human Rights Watch, the United Nations Human Rights Office Of The High Commissioner, Reporters Without Borders, Citizen Lab, and Privacy International. Applying this requirement would rule out the current German and American law enforcements' reliance on services provided by the Israeli company Cellebrite[51], as its software has

49 European Parliament Directorate-General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices STUDY

50 German Federal Office of Justice, Statistics on Telecommunication Surveillance

51 Martin Pfaffenzeller, Diese Firma knackt neue iPhones für die Kripo
Sagi Cohen, Report: Israeli company helping FBI crack iPhone security

reportedly been used against a political activist[52] and sold to entities with histories of human rights violations[53]. The same goes for Germany's current use of hacking tools provided by FinFisher[54], as the company also sold its software to – among others[55] – the Bahraini and United Arab Emirates governments, which evidently used it against activists[56]. For some countries an alternative might be to develop such tools in-house[57].

3.9 Establish a national vulnerability assessment and management process

Vulnerabilities (both known and unknown) are at the core of government hacking. Mitigating and patching vulnerabilities is crucial, however, for protecting government networks, critical infrastructures, businesses, and citizens from a wide range of attackers such as foreign intelligence agencies and cyber criminals. Therefore, assessing and managing the trade-offs and various equities of vulnerabilities is paramount for national security. Thus, a vulnerability assessment and management process should be implemented based on the framework of the Transatlantic Cyber Forum's working group on "Encryption Policy & Government Hacking"[58].

52 Sam Biddle and Fahad Desmukh, Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident

53 Joseph Cox, Cellebrite Sold Phone Hacking Tech to Repressive Regimes, Data Suggests

54 Florian Flade, Ministerium gibt neuen Bundestrojaner für den Einsatz frei

55 Morgan Marquis-Boire, Bill Marczak, Claudio Guarnieri and John Scott-Railton, You Only Click Twice - FinFisher's Global Proliferation
Claudio Guarnieri, Analysis of the FinFisher Lawful Interception Malware
Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto and Sarah McKune, Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation

56 Nicole Perlroth, Software Meant to Fight Crime Is Used to Spy on Dissidents
Nicole Perlroth, Governments Turn to Commercial Spyware to Intimidate Dissidents

57 Kevin Bankston, Ending The Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors

58 Sven Herpig, Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities

4. Operational Requirements

I. Predictable Framework

Last resort: Due to its invasiveness, government hacking operations should always be the last resort to acquire evidence that cannot be obtained through other means[59]. Before conducting a government hacking operation, law enforcement needs to exhaust all other means and document these attempts. The documentation has to be submitted as part of the warrant application process.

Applicability: The application of government hacking should mainly be focused on ex-post investigating and prosecuting crimes. In rare exceptions, in case of imminent threat of bodily harm, an ex-ante application of government hacking might be justified to protect legal rights[60].

Privileged Communication: Privileged communication (e.g. between journalists and sources and attorneys and clients) is recognized as a protected relationship that must extend to electronic communications as well, even if the data or communication is disclosed to a third party (e. g. through a cloud backup).

Preclude Legal Compulsion of ISP and Vendor Assistance: Certain government hacking operations possibly rely on the assistance of Internet Service Providers (ISP) to deliver the hacking tool[61]. A trusted relationship is needed between users and ISPs, as well as soft- and hardware vendors for cyber crime prevention; this is especially true when it comes to security updates[62]. Thus ISPs must not be legally compelled to assist in or carry out government hacking operations, for the reasons mentioned above. The same goes for

59 Privacy International, International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders
Susan Hennessey, Lawful hacking and the case for a strategic approach to “Going Dark”

60 Ulf Buermeyer, Gutachterliche Stellungnahme zur Öffentlichen Anhörung zur „Formulierungshilfe“ des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKÜ im Strafprozess Ausschuss-Drucksache 18(6)334 im Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages am 31. Mai 2017

61 Filip Kafka, Neue FinFisher-Überwachungskampagnen: Sind Internetanbieter beteiligt?

62 American Civil Liberties Union Foundation, Second ACLU Comment on the Proposed Amendment to Rule 41 Concerning “Remote Access” Searches of Electronic Storage Media Dear
Privacy International, Submission in response to Science & Technology Committee call for evidence on the draft Investigatory Powers Bill

vendors and maintainers of software, including smartphone apps and services. They must not be legally compelled to assist in delivering a malicious software or update to a target.

Access: Government hacking of a device can be conducted when having physical access to the target device or remotely. Remote government hacking operations potentially have a higher margin of error (e.g. effect on the device cannot be closely monitored, the hack might not affect the intended target, but instead another target). Additionally, remote government hacking might have IT security ramifications because devices such as smartphones are used as a second factor for authentication. Requiring physical access to the device before hacking it also more appropriately enforces the principle of proportionality of this potentially highly privacy-invasive investigatory tool. Therefore, remote government hacking should be further restricted in this way.

If all other parameters laid out in this paper are met, law enforcement should be allowed to conduct non-remote government hacking, similar to what happened in the San Bernardino[63] and Freiburg[64] cases. Remote government hacking operations must be the exception-to-the-rule and limited to investigations where physical access is not possible, such as crimes committed leveraging highly anonymized and encrypted networks[65].

Automatization: Automatized hacking operations, such as drive-by-downloads or waterholing as seen in operation "Torpedo"[66] and operation "Pacifier"[67] must only be permitted when each target is identified individually. If government hacking applies these methods, it infects or takes over a website or service and indiscriminately delivers malware to every visitor and user of that website or service. Government hacking operations always need to be targeted and those targets need to be specifically named in the warrant[68], for example by the name of the device and owner or a technical identifier (such

63 Ellen Nakashima, FBI paid professional hackers one-time fee to crack San Bernardino iPhone

64 Katharina Kutsche und Hakan Tanriverdi, Wie Polizisten das Handy des Tatverdächtigen auslasen

65 Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

66 Kevin Poulsen, Visit the Wrong Website, and the FBI Could End Up in Your Computer

67 Sven Herpig, Government Hacking: Computer Security vs. Investigative Powers

68 European Parliament Directorate-General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices STUDY

as an IMEI[69], phone number or account name) in cases where the owner is unknown. Additional limitations apply (see "access"). The risks of potential dragnet collection and endangering third parties might outweigh the operational value of the information obtained.

II. Privacy and Security

Privacy: Data collected by government hacking but not relevant for the prosecution of a crime needs to be deleted immediately to ensure maximum possible privacy protection[70]. Deletion of this data has to be conducted with state-of-the-art software to ensure that this data cannot be restored. The fact that information was collected and deleted needs to be logged.

Sensors: Devices such as smartphones, tablets and home automation systems are increasingly equipped with a number of sensors ranging from (video) cameras to biometric sensors, GPSs, accelerometers, gyroscopes, barometers and more. Access to those sensors and the ability to manipulate them are powerful - and cheap[71] - tools in investigations, but simultaneously reveal an incredible amount of private information about its user. This is especially true because if accessed by law enforcement, sensorial data will be generated and/ or stored which would have otherwise not have been done by the user. Therefore, government hacking leading to access to sensors must be tied to specifications in the super-warrant (see "warrants") and is further limited by the restrictions on remote government hacking (see "access"). Audio-optical sensor access must be further limited to space outside the core area of private life[72], for example by geo-fencing[73], a technique that allows and disallows functions based on the geolocation of the device.

Vulnerabilities: The 2016 security review by Google has shown that only half of the top 50 Android phones have received the current security updates[74].

69 techopedia, International Mobile Equipment Identity (IMEI)

70 European Parliament Directorate-General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices STUDY

71 Kevin S. Bankston and Ashkan Soltani, Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones

72 The core area of private life [German: "Kernbereich privater Lebensgestaltung"] is for example by German jurisprudence defined as the physical space of your home which cannot be targeted by certain surveillance mechanisms.
Bundesverfassungsgericht, Leitsätze zum Urteil des Ersten Senats vom 3. März 2004 - 1 BvR 2378/98 - - 1 BvR 1084/99

73 SPIEGEL Online, Spionagesoftware Skygofree liest WhatsApp mit

74 Android Security 2016 Year In Review

Adding the many end-of-lifecycle devices (those which do no longer receive patches) – to this equation, the number of non-patched smartphone devices with known vulnerabilities becomes extremely high. Acquiring and retaining unknown vulnerabilities comes with an extensive set of critical challenges (commerce, IT security, civil liberties etc.) for the government[75]. Additionally, exploiting an unknown vulnerability always carries the risk of exposure, and therefore degradation of its operational value. Thus, government hacking should be limited to the use of known vulnerabilities.

Data security: Data obtained through government hacking possibly includes a large amount of sensitive and private information and therefore needs appropriate safeguards. To maintain the data's security, it must be protected by state-of-the-art tools and measures ("Stand der Technik")[76]. Furthermore, the general standards for data retention applicable to the country need to be complied with.

Hacking tools: In order to maintain the integrity of the digital evidence that is extracted from the target's device, hacking tools need to be secured in line with state-of-the-art guidelines, which include penetration testing. The tools also need to be thoroughly developed and tested so that they do not cause malfunctions[77], such as accidentally destroying evidence. Additionally, they must be equipped with a tamperproof logging mechanism, allowing judiciary and others to retrace and comprehend the investigation. These safeguards are not only aimed at preventing accidental corruption of digital evidence, but also at protecting the target from the planting of evidence[78] or the exploitation of the evidence for other purposes. Evidence suggests that government hacking and surveillance tools have oftentimes not fulfilled those requirements[79].

75 Sven Herpig, Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities

76 Oliver Schonschek, Was Stand der Technik in der DSGVO bedeutet

77 The Internet blackout in Syria is an example of a government hack gone wrong. Though it was not a domestic government hacking or surveillance tool, the US National Security Agency accidentally caused the blackout while trying to conduct a cyber espionage operation.
Spencer Ackerman, Snowden: NSA accidentally caused Syria's internet blackout in 2012

78 Privacy International, International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders

79 Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark and Matt Blaze, Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps
Chaos Computer Club, Chaos Computer Club analyzes government malware
Dan Goodin, Root backdoor found in surveillance gear used by law enforcement

III. Judicial Oversight[80]

Warrants: Government hacking operations are not only highly invasive but can also lead to massive dragnet data collection, for example collection of personal information from people who are affiliated with the target (messenger histories, pictures, etc. on the hacked device), but also those who have nothing to do with the crime that is being investigated. Therefore, a high standard of judicial oversight is required. The requirement for government hacking operations by law enforcement should therefore be an ex-ante[81] "super-warrant"[82]. The warrant would have to be obtained before the beginning or continuation of a government hacking operation, and would need to mention all of the apps, data and sensors it targets. In addition, it needs to state the duration of the operation as well as the the soft- and hardware used by law enforcement, potential risks to security of the systems, and a statement that all ordinary investigative techniques have failed or would be ineffective. The warrant expires after three months. To extend the warrant beyond three months, a new approval is required[83].

Notice: To facilitate remedial actions, all government hacking operations must include a notification of the target of the operation and, when applicable, also to all owners of the devices impacted[84]. The notification needs to include the particularity requirements laid out in the warrant application. Due to operational concerns, the notice does not have to be provided before or during an ongoing government hacking operation, but within 90 days after the end of the operation. The notice must include further information, and an explanation of the remedy mechanism (e.g. the legal framework and possible points of contact). An ex-post facto notice "facilitates transparency

80 Kerr and Murphy state that in addition to judicial oversight, "law enforcement has every incentive to subject decisions to use NITs to extensive oversight within the executive branch".
Orin S. Kerr and Sean D. Murphy, Government Hacking to Light the Dark Web

81 Ex-ante judicial authorization is standard in many EU countries, including France, Germany, Italy, the Netherlands, Poland, and the United Kingdom.
European Parliament Directorate-General for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices STUDY.

82 Jonathan Mayer, Government Hacking referencing Berger v. New York

83 One of the several aspects in this paper which is already enshrined in German law.
Bundesministerium der Justiz und für Verbraucherschutz, Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Artikel 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) (Bundeskriminalamtgesetz - BKAG) § 20k Verdeckter Eingriff in informationstechnische Systeme.

84 Amie Stepanovich, A Human Rights Response To Government Hacking

and promotes confidence in government investigative practices that do not involve ex-ante notice, ensuring that law enforcement officers comply with legal constraints"[85].

Disclosure: The vulnerability itself which was used in the government hacking operation might have little value to the defense in a criminal investigation[86]. However, combined with the soft- and hardware that was used for the operation, it could tamper with the integrity of the evidence. Therefore, the soft- and hardware (including the vulnerability used) should be audited by an independent outside expert under a confidentiality agreement. The prosecution must disclose in court, however, the attack vector and the method (e.g. brute force, malware using a known vulnerability) of the operation, which devices were targeted, and, of course, what digital evidence was accessed. Disclosure of this information enables other actors, including the defense counsel, to make a case about whether the evidence could have been planted there by a third party and/or could be used as a way of measuring whether the evidence could have been obtained by alternative measures.

85 Jonathan Mayer, Government Hacking referencing Brian L. Owsley, To Unseal or Not To Unseal: The Judiciary's Role in Preventing Transparency in Electronic Surveillance Applications and Orders

86 Susan Hennessey and Nicholas Weaver, A Judicial Framework for Evaluating Network Investigative Techniques

Operational Requirement	
Last Resort	*Yes, papertrail that all other means have been exhausted.*
Applicability	*Ex-post facto application.* *Ex-ante application limited to rare exceptions (imminent threat of bodily harm).*
Privileged Communication	*Special protections apply.*
Preclude Legal Compulsion of ISP and Vendor Assistance:	*Internet Service Providers and soft- and hardware vendors must not be mandated to assist in government hacking operations.*
Access	*Physical access to the device required.* *Remote government hacking only permitted in investigations where non-remote is not possible.*
Automatization	*Automatized government hacking only if tied to previously approved (warrant) personal or technical identifiers and limited by additional restrictions.*
Privacy	*Immediately delete non-relevant collected data with state-of-the-art software.*
Sensors	*Linked to specifications in the warrant and further limitations.* *Audio-visual sensors additionally limited to outside the core area of private life.*
Vulnerabilities	*Should be limited to known vulnerabilities.*
Data Security	*Must be protected by state-of-the-art tools and measures and follow existing data retention laws and regulations.*
Hacking Tools	*Need to be securely and thoroughly developed, tested and be equipped with tamperproof logging mechanism.*
Warrant	*Ex-ante "super warrant", maximum of 3 months, renewal possible.*
Notification	*Ex-post facto notification.*
Disclosure	*Only modus operandi in court but independent expert audit of the entire operation, including vulnerability exploited.*

Table 1. Overview "Operational Requirements"

5. Conclusion

The ongoing debate about the "going dark" challenge and its implications is unlikely to go away. Whereas government hacking has been identified as one possible solution, in some places[87] the political debate reverts to a repetition of familiar discredited arguments. Weakening encryption, mandating an encryption regime, or compelling backdoors are approaches that are doomed to fail; most experts working at the intersection of national security, privacy and IT security have acknowledged this conclusion[88]. It is therefore not only forward-looking but also imperative to come up with a framework that might resolve this key challenge and move the debate beyond the old battlelines. The suggested requirements for government hacking shall serve as a practical guideline for states to balance their preventive and investigatory requirements with the inherent security and privacy needs arising from hacking-backed surveillance. When applying the aforementioned guidelines, it is crucial to apply as many aspects as possible and not to resort to cherry picking. Only after all aspects are considered and implemented might the right balance be achieved. Concurrently, more empirical research must be conducted with regards to the real extent of the "going dark" challenge and its implications for law enforcement, as well as with regards to alternative solutions for solving this challenge.

87 EastWest Institute, Encryption Policy in Democratic Regimes

88 Transatlantic Cyber Forum, Initial Take-Away: Encryption Policy and "Government Hacking"

This analysis has been supported by members of the Transatlantic Cyber Forum through online collaboration and joint workshops in Washington D. C. and Berlin. The views and opinions expressed in this paper are those of the author and do not necessarily reflect the official policy or position of the working group members or that of their respective employer/s.
Acknowledging essential contributions of:

1. Cathleen Berger, Mozilla
2. Ulf Buermeyer, Gesellschaft für Freiheitsrechte (GFF)
3. Betsy Cooper, independent
4. Marc Fliehe, VdTÜV - Association of Technical Inspection Agencies
5. Sharon Bradford Franklin, New America's Open Technology Institute
6. Ernst Härtl, Digital4TRESS
7. Karsten König, CIPHRON
8. Andreas Kuehn, EastWest Institute
9. Susan Landau, Tufts University (affiliation for identification purposes only)
10. Daniel Moßbrucker, Reporters Without Borders Germany
11. Holger Muehlbauer, TeleTrusT - IT Security Association Germany
12. Riana Pfefferkorn, Center for Internet and Society, Stanford Law School
13. Thomas Reinhold, Institute for Peace Research and Security Policy Hamburg/ cyber-peace.org
14. Michelle Richardson, Center for Democracy and Technology
15. Julia Schütze, Stiftung Neue Verantwortung
16. Christoph Zurheide, Deutsche Post DHL Group

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organisation adopted a concept of mixed funding sources that include foundations, public funds and businesses.

Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organise conferences that address these issues and further subject areas.

About the Transatlantic Cyber Forum (TCF)

The Transatlantic Cyber Forum (TCF) has been established by the Berlin based think tank Stiftung Neue Verantwortung (SNV). The SNV is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state.

The Transatlantic Cyber Forum is a network of cyber security experts and practitioners from civil society, academia and private sector. It was made possible with the financial support from the Robert Bosch Stiftung and the William and Flora Hewlett Foundation.

About the Author

Sven Herpig is the project director of the Transatlantic Cyber Forum (TCF), bringing together American, German and other EU-experts to collaborate on cyber security policies.

How to Contact the Author

Dr. Sven Herpig
Head of International Cyber Security Policy
sherpig@stiftung-nv.de
Twitter: @z_edian
+49 (0)30 81 45 03 78 91

Imprint

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de