January 2018 · Dr. Sven Herpig

Government Hacking

Global Challenges

Stiftung Neue Verantwortung

Think Tank at the intersection of technology and society

Executive Summary

Since the first crypto war of the 1990s[1], governments have tried to square the seeming ambivalence of encryption. While it enables secure communications which is vital for the economy and the government itself[2], it also allows criminals to easily hide their communication and data from law enforcement – the so-called "going dark" challenge. Over the years, there have been numerous approaches and proposals[3] to tackle this issue, such as government mandated backdoors, weakening of encryption standards[4] and direct access[5]. Experts across the board however agree that "strong encryption is the basis for secure digital communications and, consequently, that weakening encryption or requiring providers of encrypted products or services to redesign their offerings in order to facilitate government access[6] is detrimental to national security. Therefore, several countries – among them Germany and the United States[7] – have taken to enabling law enforcement and intelligence agencies to conduct investigations via hacking tools (referred to as "government hacking") in order to shine a light into the going dark problem. Government hacking is not without its shortcomings, to say the least. Neither have those challenges been addressed in an orderly manner, nor have other alternatives – apart from those mentioned above – been thoroughly discussed[8]. Those aspects form the scope for this overview. A clear legal and policy framework for government hacking[9] is needed to

1 https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/

2 https://static.newamerica.org/attachments/3407--125/Lessons%20From%20the%20Crypto%20Wars%20of%20the%201990s.882d6156dc194187a5fa51b14d55234f.pdf

3 https://www.newamerica.org/cybersecurity-initiative/policy-papers/brief-history-law-enforcement-hacking-united-states/

4 https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/

5 https://www.nap.edu/catalog/23593/exploring-encryption-and-potential-mechanisms-for-authorized-government-access-to-plaintext

6 https://www.stiftung-nv.de/sites/default/files/tcf-encryptionpolicy_governmenthacking.pdf

7 https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

8 https://edri.org/files/encryption/workarounds_edriposition_20170912.pdf, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2938033 and https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

9 Throughout the paper, there will be several references to German laws and discussions. Germany has developed its legal framework for government hacking

address these challenges thus minimizing privacy violations and limiting overall weakening of informational security. Developing such a framework however requires an identification of the core problems of government hacking. The challenges of the going dark problem set, encryption or government hacking[10] do not stop at national borders. Therefore, fostering a common understanding and sharing best practices within a multilateral or transnational approach might yield significant progress towards solving the core challenges. Those challenges are[11]:

1. Developing a predictable framework;
2. Maximizing privacy and minimizing security impact;
3. Adopting clearly defined legal standards;
4. Respecting international law and considering international implications;
5. Establishing balanced oversight and transparency;
6. Exploring alternative solutions;
7. Developing a vulnerability management system.

over the last couple years which consequently led to many political and legal debates regarding this issue. Thus, there are several positive and negative aspects of this debate that function as points for this paper.

10 https://motherboard.vice.com/en_us/article/53d4n8/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant

11 https://www.stiftung-nv.de/de/veranstaltung/transatlantic-cyber-forum-track-1-experts-met-dc-workshop

1. Defining the Playing Field: "Government Hacking"

Before diving into the analysis of challenges that government hacking poses, it is worthwhile to have a common understanding of the terminology used. Government hacking has been mainly used to describe two different activities. One is the conduct of cyber operations against foreign states and the other one is the use of cyber operations for law enforcement purposes. The latter definition is applied here.

While government hacking has mainly been mentioned within the context of the encryption debate, it also goes beyond it. Government hacking can also be applied to devices which do not use encryption but are for example protected by other security mechanisms. What government hacking refers to is the government's exploitation of existing vulnerabilities in software and hardware to access the plaintext of data in transit and data at rest or manipulate a target's device (e. g. switching on sensors or webcams). Government-developed malicious software - such as a Trojan Horse - can be installed on a target's device either remotely through government hacking or through gaining physical access to the device itself. In the latter case, the government might not even need to exploit a vulnerability to install its malware or access data on the device. Knowing the passcode for example would allow Law Enforcement Agencies (LEA) to access information on the device without exploiting a vulnerability. The remote installation can be conducted via spear phishing, a method also used by criminals and intelligence agencies, or through cooperation with tech companies and Internet service providers[12].

If governments want to implement government hacking efficiently without vast privacy intrusions and or weakening encryption protocols, they must solve a number of challenges intrinsic to government hacking. Tackling those challenges leads to a prudent framework for government hacking. As a first step, those challenges need to be defined, which is the core task of this paper.

12 https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

2. Challenges for Government Hacking

2.1 Developing a predictable framework

a) Ex-ante versus ex-post

An initial decision that has to be made when discussing government hacking is its strategic purpose in the realm of law enforcement. The first step is therefore to decide whether government hacking should be restricted to the prevention[13] of crimes (ex-ante) to avert danger or also be applied to prosecute[14] them when they already took place (ex-post). By allowing only ex-ante application, it limits the extent of government hacking in certain cases substantially. However, this is not a blanket decision and can depend for example on the seriousness of the crime.

b) Seriousness of the crime

The seriousness of the crime for which government should be allowed to conduct hacking is a vital consideration. Enabling an agency to conduct hacking for a criminal investigation should depend also on the crimes it is used to avert or prosecute. For drafting a clearly defined government hacking framework would mean to either list those crimes individually or categorically[15]. Again, this needs a differentiated debate based not only on an ex-ante/ex-post framework used in 2.1 a), but also on other aspects such as the invasiveness of government hacking discussed in 2.2.

c) Targeted versus bulk

Another consideration which needs to be discussed in order to come up with a solid government hacking framework is whether it will be conducted as a targeted operation only or in bulk as well. While a targeted operation might have a higher level of quality control and assurance, bulk government hacking[16] can potentially have unforeseen domestic and international consequences.

13 German: “Gefahrenabwehr”

14 German: “Strafverfolgung”

15 An example can be derived from the German legal provisions on government hacking. They allow the application of government hacking for “serious crimes” [German: “schwere Straftaten] and subsequently lists those crimes, compare §100a (2) code of criminal procedure [German: “StPO"].

16 An example for bulk hacking is “Operation Pacifier” which was conducted by the FBI, compare: https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

d) Level of automatisation

Closely connected to government hacking in bulk is the level of automatisation. A high degree of automatisation[17] in government hacking might lead to more efficiency but also bears the potential for unintended consequences and less diligence. Whether the level of automatisation is an essential condition for government hacking also depends on the application of it, whether it is conducted remotely or locally.

f) Remote versus local

The distinction between remote government hacking and local government hacking[18] is closely interlinked with several aspects of this paper. Local hacking would require a prior action such as search and seizure and would not work against criminals which are only known online as stated in 2.2 g). As with many other of the aspects mentioned previously it can be applied in a leveled approach - for example remote is only permitted in "darknet" investigations - and therefore limit the scope of government hacking.

g) "Last resort"

Section 2.6 discusses alternatives to government hacking. In certain instances, or for certain crimes, such as (cyber) crimes committed via the darknet, government hacking might be the only way to either prevent the crime or gather evidence of the crime to identify and persecute the criminals. This so-called "last resort" might be considered as a strong predicate for government hacking, meaning that all other means have to be exhausted before government hacking will be permitted.

h) Human resources

The increase of overall cyber experience adds value to the predictability of a framework. The need - and shortage - of technically skilled staff that is willing to work for the public sector needs to be factored in. Whereas government hacking is hailed as a highly efficient way of conducting investigations, it ignores the fiscal and manpower constraints that governments face. Education, training and staff developed are crucial to maintain a workforce

17 An example for a high level of automatisation in government hacking is "Operation Pacifier" which was conducted by the FBI, compare: https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

18 Local government hacking refers to having physical access to the information system before hacking it (San Bernardino iPhone case) as compared to remote hacking as seen during Operation Pacifier. More details about the San Bernardino case: https://www.wired.com/2016/04/fbi-hints-paid-hackers-1-million-get-san-bernardino-iphone/

that is capable of conducting those kinds of operations.

2.2 Maximizing privacy and minimizing security impact

a) Data in transit and data at rest

A vital distinction to limit the extent of privacy intervention should be made between accessing data in transit and data at rest. Data in transit would for example include messages on a smartphone before being encrypted and subsequently transmitted whereas data at rest would include all data existing on a device. The difference in the level of privacy intrusion has led Germany's policy-makers to differentiate between the two in its recent legal amendment[19]. However, clearly defining the two will continue to be a challenge for governments[20].

b) Limiting access

Allowing either access to data in transit or at rest could be another blanket provision. Within those categories, access could be limited to certain apps, sensors, camera, multimedia files, messengers to name a few.

c) Core area of private life[21]

An even more nuanced way of limiting access of government hacking tools could be based on issues such as the core area of private life. That would for example mean that investigators could access data in transit and at rest, including sensors and cameras, but only if the GPS signal does not indicate that the surveillance target is in his/ her bedroom. Access could also be limited to exclude certain communication partners such as spouses or those offering the protection of client privilege.

d) Data protection

Data retention and security guidelines for the data obtained from the targets of government hacking are vital to limit privacy intrusions. How long data should be retained for, who can access it and for what purpose, how is it

19 https://www.bundestag.de/dokumente/textarchiv/2017/kw25-de-aenderung-stgb/511182

20 http://www.freilaw.de/wordpress/wp-content/uploads/2017/05/08Pretz_Telekommunikations%C3%BCberwachung.pdf

21 The core area of private life [German: "Kernbereich privater Lebensführung"] is for example by German jurisprudence defined as the physical space of your home which cannot be targeted with certain surveillance, see mechanisms. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2004/03/rs20040303_1bvr237898.html

secured against third parties, how is its integrity maintained, and what standards should apply for deletion of that data, are all considerations that need to be taken into account.

e) Secure hacking tools

To maintain the security and privacy of a suspect's device, the hacking tools used by the investigators need to be secure. If third parties could exploit devices because they have been hacked by government investigators due to insecure hacking tools[22], it could have serious consequences for the suspect as it leaves them vulnerable to exploitation by criminal and intelligence agency actors. This vulnerability is further outlined in the topic of "planting evidence".

f) Test hacking tools

Similar to e), hacking tools have also to be thoroughly tested to not render systems useless ("bricking" them) or otherwise cause unintentional damage, such as erasing/ tampering with potential evidence on target devices.

g) Notification of target

Another crucial point of discussion is, if and when a target of government hacking will be informed about the investigation. By not informing a target about a devices weaknesses, investigators indirectly become complicit if cyber criminals exploit the vulnerability.

h) Known versus unknown vulnerabilities

Allowing government agencies to use unknown vulnerabilities without disclosing them leads to a decrease in the overall degree of national (cyber) security. This can lead to those vulnerabilities potentially being exploited by belligerent actors against government officials (such as soldiers[23]), company employees, and its own citizens, thereby enabling political and economic espionage as well as cyber crime more broadly[24]. See also 2.7.

22 While one of the German law enforcenment agencies was developing its own hacking tool, the purely defensive national cyber security was commanded by the Ministry of Interior to support the LEA, see https://www.heise.de/newsticker/meldung/Geheimpapiere-BSI-entwickelte-Bundestrojaner-mit-2577582.html

23 https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402

24 https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

2.3 Adopting clearly defined legal standards

a) Warrants

After an U.S. federal judge signed off on a warrant that would allow the FBI to use a server in the judge's district to automatically hack everyone accessing the portal hosted on that server, a debate started whether this would be covered by the applied Rule 41[25]. In the FBI case, Operation Pacifier, thousands of computers worldwide were hacked based on this single warrant. Later, a legal amendment[26] to Rule 41 clarified that this was indeed legal. The clarity and extent of a warrant is of utmost importance in the realm of government hacking as it possibly transcends borders and leads to bulk hacking. The scope that a warrant allows, investigators, is closely connected to other challenges mentioned in this paper, especially 2.2 g) and h).

b) Disclosure in court

Another challenge is the amount of technical and procedural details that need to be disclosed in court to enable judge and defense council to make informed decisions and arguments. While it does not seem necessary to disclose the vulnerability in court - if addressed adequately as discussed later in this paper - details about the hack and the used tool should be disclosed to judge and defense council. It enables the parties to see for example if the chain of custody was maintained and whether or not the warrant was correctly adopted. The disclosure also has to factor in 3rd party involvement to prevent circumvention of disclosure regulations[27].

c) Capacity building

The entire judicial staff (prosecutors, judges and defense council) needs to receive the appropriate training to understand the complex issue of government hacking. Further still, judicial staff must have a basic understanding of the technical aspects of the cases they are presented. Capacity building is especially important as it pertains to the legality of government hacking. This can range from the integrity of the digital chain

25 https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

26 http://fortune.com/2016/11/30/rule-41/

27 When the FBI procured the services of a private contractor to hack the iPhone of Syed Farook. Instead the FBI did not hand over the used vulnerability instead stating it procured the service (and possibly a tool) from a 3rd party but never acquired knowledge concerning the vulnerability itself, see https://www.washingtonpost.com/world/national-security/fbi-wont-reveal-method-for-cracking-san-bernardino-iphone/2016/04/26/d6d66126-0bc3-11e6-bfa1-4efa856caf2a_story.html

of evidence, digital signing, and how the security of devices in question are relevant to legal proceedings. The judiciary needs to be equipped with this understanding to make prudent, informed decisions.

d) Integrity of evidence

Linked to 2.2 e) and f) is the issue of maintaining the integrity of electronic evidence and the chain of evidence[28]. Generally speaking, maintaining the integrity is nothing new as it is also crucial for conventional investigations. However, with government hacking and electronic evidence, there are new challenges to consider such as digital signing (of evidence), encrypted data transfer as well as the (in)security of the target device. If those technical considerations are addressed appropriately, electronic evidence can be tampered with.

e) 3rd party manipulation

Closely related to the integrity of evidence is the integrity of the target devices and subsequently the issue of planting evidence. If the investigators can access those devices, so can (potentially) criminals and foreign intelligence services. Planting digital evidence has to be factored in judicial proceedings similarly to how planting evidence is considered in "non-digital" investigations. Cyber criminals and intelligence agencies use compromised third party IT-systems to stow away their data and/ or to obfuscate their tracks[29].

2.4 Respecting international law and considering international implications

a) International legal, practice and normative spillover

There is no truly national legislation in cyberspace. Not only because everything is connected and the same technology is used everywhere, but also due legislation possibly causing a myriad of unintended spillover effects. During the Brazilian legal case about blocking Facebook's messaging service WhatsApp[30] both, government and civil society, were looking at

28 The German legal framework that covers government hacking https://www.gesetze-im-internet.de/bkag_1997/__20k.html

29 E. g. a British company alerted Germany's domestic intelligence agency, that it had found documents stemming from its parliament on their servers, see https://www.stiftung-nv.de/sites/default/files/tcf-defending_political_lt-infrastructures-problem_analysis.pdf

30 https://www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html

the arguments of the recently passed government hacking amendment in Germany. In another case, the Russian Duma adopted a recently passed German hate speech law. This led to the NGO Reporters without Borders stating: "The German law on online hate speech is now serving as a model for non-democratic states to limit Internet debate"[31]. It is therefore imperative to at least consider possible spillover effects of laws, legislation, and practices that are enacted, especially when it comes to acquiring vulnerabilities and hacking tools.

b) Human rights framework

Although referring to a third party state, the 2011 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue) clearly states that "[w]hen a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression"[32]. While inherent to several of the aspects mentioned here (for example 2.2 c) and g), 2.3 e), 2.4 d) and 2.6 b)), it is essential to underline again, that any government hacking activity undertaken by a state against its citizens and possibly citizens of other countries (see 2.1 c) and2.4 c)) needs to adhere to the human rights framework[33].

c) Sovereignty violations

Operation Pacifier has shown, that criminal investigations utilizing hacking tools can easily violate sovereignty of other countries[34]. However, it seems as long as the LEA's share their findings with their international counterparts, cooperation agreements are strong enough on an operational level to not spark international conflict[35]. This however does not mean that it will not be a challenge in the future, something which needs to be tackled on an international level. Possible safeguards could be to restrict cross border government hacking to the use of beacons (sending back location of the target) only. Another option would be to design the hacking tools in a way that they automatically filter foreign IPs - even beyond VPNs/proxies - before

31 https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law

32 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

33 https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

34 https://www.stiftung-nv.de/de/publikation/government-hacking-computer-security-vs-investigative-powers

35 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2957361

storing them. Even though these options would make the outcome of a government hacking operation less invasive, the cross border hacking of computer systems outside of the law enforcement jurisdictions would still have taken place.

d) Remedy mechanisms

Government hacking needs to recognize that human rights violations might occur during the process of an operation. Therefore, states have to provide legal remedy mechanisms for such cases to be resolved on the national and international level[36].

2.5 Establishing balanced oversight and transparency

a) Transparency report

Transparency is an aspect that needs to be considered when discussing government hacking. An annual transparency report (federal and state level) is a key requirement towards accountability and should be based on empirical evidence on the application of government hacking. The German government hacking framework for example requires protocoling of its law enforcement activities[37]. Out of this data the Federal Office of Justice creates an annual transparency report[38].

b) Track normative spillover and sovereignty violations

An non-essential but useful element of a prudent government hacking approach is the tracking of normative spillover effects (see 2.4 a)) and sovereignty violations (see 2.4 c)). Having this data available allows to improve the government hacking framework to better tackle those challenges.

36 http://www.ohchr.org/EN/ProfessionalInterest/Pages/RemedyAndReparation.aspx and https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf

37 For example protocoling the means used, the date, the description of the target system and all changes done to it, information about the data which was collected and the organisation that carried out this activity. The legal framework can be found in the German Code of Criminal Procedure (StPO) §100a-g, revised after June 2017.

38 Including the number of activities per year, new activities and extensions, reasons and crime for the activity, if the target has been informed about it or not, if significant evidence was found or not, what resources have been spent and if 3rd parties were targeted in the process. See: https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung_node.html

c) Parliamentary and judicial oversight

Depending on the nature and target of the operation, either parliamentary or judicial oversight needs to be in place. The independent oversight body needs to be equipped with sufficient resources to make informed decisions. The staff's expertise (see 2.3 c)) is of utmost importance due to the technical sophistication of this field. This is also due to the considerable implications government hacking has on international relations.

2.6 Exploring alternative solutions

a) Needs assessment

A comprehensive needs assessment based on the above mentioned empirical data should be the starting point for creating any government hacking framework. As shown throughout this paper, a prudent approach requires not only time and resources but faces many challenges. This assessment also has to factor in alternatives to government hacking which have not yet been fully explored. An in-depth assessment can be beneficial to customize investigative methods and increase their effectiveness by going beyond a "catch-all" government hacking approach.

b) Proportionality

Depending on the type of operation (see 2.2), government hacking can be very invasive to individual freedoms. Therefore, it is fundamental to consider less invasive alternatives of investigation before resorting to government hacking. As mentioned in 2.1 g) government hacking can be the last resort, but this assumption has to follow a methodology or framework.

c) Trove of information

The challenge of "going dark" is always considered a severely limiting factor for the information that LEA's have access to. While that might be true, the digitization allows those same stakeholders to have access to a wide variety of information they might of not had access to in the past. This includes information on social media accounts, GPS data, telemetry and metadata as well as video surveillance footage among others. Arguably, there is more information about the targets of investigations available to law enforcement than ever before. Weighing the invasiveness of government hacking, it might be more efficient to improve communication, collection methods, and evaluating information already gathered than adding another instrument to the toolbox.

d) Conventional methods

Utilizing and improving conventional methods for investigations such as observations, search and seizure or undercover operations - enhanced with the new trove of information (see 2.6 c)) - could possibly deliver better results and sufficient evidence, despite the going dark of criminals. A successful example that combines several traditional investigatory methods where no government hacking was required is the takedown of the drug portal known as the Silk Road[39]. Although requiring more human resources this is but one part of the equation, as invasiveness and a shortage of human resources (see 2.1 h)) add downward pressure to the problem set.

e) Special use cases

One of the main arguments for government hacking is its use to conduct investigations on the darknet. While there have been several success stories (for example Operation Pacifier), there have also been success stories of darknet takedowns which did not require government hacking (for example Silk Road). Following this argument, special use cases can be created to simultaneously enable government hacking and limit its scope. One of those cases could be to limit government hacking to the application of beacons to support darknet investigations only.

2.7 Developing a vulnerability management system

a) Defining vulnerabilities

Successful government hacking activities might rely on a vulnerability that can be exploited to gain access to data. For the scope of this paper, a vulnerability is defined as a flaw in soft- or hardware which individually or chained with others enables third parties to perform unauthorized - and possibly covert - operations on a device or against a digital account. There are two categories of vulnerabilities, those which are already known by the manufacturer (n-days/ “old days”) and those unknown to it (0-days / “oh days”). The process leading from a 0-day to a n-day is referred to as disclosure. Although n-days have been disclosed to the manufacturer, they might not be fixed - and in some cases, will never be fixed. Even if a vulnerability is disclosed and fixed, it does not mean that LEAs/Intelligence Community (IC) cannot exploit it anymore. The user of the respective system often still has to actively trigger the update which patches the vulnerability. If the user does not do that, LEAs/IC can still exploit it. A recent study concluded that most

39 https://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/

hacking attacks in 2015 exploited n-days which had fixes readily available[40].

b) Institutionalizing vulnerability management

Vulnerability management is a complex topic which needs dedicated research, and which is currently being conducted inter alia by the working group on "encryption policy & government hacking"[41] of the Transatlantic Cyber Forum. A holistic approach needs to tackle procurement, evaluation and responsible disclosure of vulnerabilities. Each of those categories comes with its own set of challenges[42]. The American Vulnerabilities Equities Process (VEP)[43] and the German setup of its Central Authority for Information Technology in the Security Sphere (ZITiS)[44] shows that a dedicated institution for national vulnerability management is a step in the right direction to avoid redundant structures.

c) Vulnerability categories

As mentioned in 2.7 a), n-day vulnerabilities might be enough to conduct government hacking. A government hacking framework needs to consider whether it sticks with n-days or extends itself to 0-days. Due to several aspects mentioned in this paper (for example 2.3 b), 2.5 a) and 2.7b)), the inclusion of 0-days for criminal investigations would create an even bigger challenge.

40 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

41 https://www.stiftung-nv.de/en/project/international-cyber-security-policy#erstens

42 Among others: where and from whom to buy vulnerabilities and hacking tools, what aspects to factor in when doing the evaluation of a vulnerability, how strong should the disclosure bias be, if a vulnerability is retained after what time should it be re-evaluated.

43 https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF

44 https://www.zitis.bund.de/DE/Home/home_node.html

3. Conclusion

In summary, this paper tries to provide a conclusive overview about the challenges that governments face when creating a predictable government hacking framework. The main challenge which can be derived from this assessment is that there cannot be a binary approach to government hacking. The myriad of challenges that need to be considered in different situations shows that there is no one-size-fits-all approach. Creating a corresponding model for an "indicator of invasiveness" could be a next step.
On a more strategic level, governments have to come up with solutions to many of these problem sets - such as the security of hacking tools, staff shortages, vulnerability management - before even engaging in government hacking. Creating such a framework can be done through multilateral cooperation by looking at best practices and lessons learned across such a cooperation. Apart from these examples, research is needed in several fields such as alternative methods and information sources (e. g. Metadata, sensor-data), spillover effects, rates of vulnerabilities and empirical evidence of government hacking operations which provided substantial evidence and where no alternative to it was available (sine qua non condition).

As shown in the case studies cited in this paper, governments have already started, or will shortly, to adopt government hacking tactics for their criminal investigations. The research that is needed to produce smart policy recommendations needs to incorporate already existing individual frameworks and their effects. Much research will only be finalized after those countries already adopted their individual frameworks. It is therefore essential to - where possible - conduct continual review and include a sunset clause that would allow for substantial revisions based on those findings.

In closing, government hacking is not "only" about national security versus privacy and human rights. It is also about public security versus information security, where the latter is quintessential for the former. It comes down to the question of whether we can come up with a prudent and holistic government hacking framework that respects the right to privacy and human rights. This framework must strike a balance between enhancing privacy protection and also enabling LEA's to carry out the necessary work that they do. Simply enabling sweeping government hacking powers because criminals are "going dark" and governments have the capabilities is not only bad practice but fails to address many of the challenges presented in this paper.

About 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.

The experts of the SNV formulate analyses, develop policy proposals and organise conferences that address issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance and further subject areas.

The SNV established a new working method for the development of policy proposals. Academic expertise provides the basis. The SNV however systematically involves and co-operates with experts in the fields of politics, economy, NGOs and research institutes and this already at an early stage in the process in order to rapidly test and improve policy proposals. This collaborative working method allows for different perspectives to participate in the process, inoperative proposals to be discarded early and ideas to be made practicable.

About the Transatlantic Cyber Forum

The Transatlantic Cyber Forum (TCF) has been established by the Berlin-based think tank Stiftung Neue Verantwortung (SNV). The TCF was made possible by the financial support of the Robert Bosch Stiftung and the William and Flora Hewlett Foundation.

TCF is an intersectoral network of experts from civil society, academia and private sector working in various areas of transatlantic cyber security and cyber defense policy. It currently consists of three working groups with more than 90 experts.

More information about the project can be found on https://www.stiftung-nv.de/en/project/international-cyber-security-policy

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