Accountability and the Canadian Government's Reporting of Computer Vulnerabilities and Exploits

By Christopher Parsons[1]

Abstract:
Computer security vulnerabilities can be exploited by unauthorized parties to affect targeted systems contrary to the preferences their owner or controller. Companies routinely issue patches to remediate the vulnerabilities after learning that the vulnerabilities exist. However, these flaws are sometimes obtained, used, and kept secret by government actors, who assert that revealing vulnerabilities would undermine intelligence, security, or law enforcement operations. This paper argues that a publicly visible accountability regime is needed to control the discovery, purchase, use, and reporting of computer exploits by Canadian government actors for two reasons. First, because when utilized by Canadian state actors the vulnerabilities could be leveraged to deeply intrude into the private lives of citizens, and legislative precedent indicates that such intrusions should be carefully regulated so that the legislature can hold the government to account. Second, because the vulnerabilities underlying any exploits could be discovered or used by a range of hostile operators to subsequently threaten Canadian citizens' and residents' of Canada personal security or the integrity of democratic institutions. On these bases, it is of high importance that the government of Canada formally develop, publish, and act according to an accountability regime that would regulate its agencies' exploitation of computer vulnerabilities.

Version: 1.2.1
Dated: Nov 2, 2018

---

[1] Dr. Christopher Parsons a Research Associate at the Citizen Lab, in the Munk School of Global Affairs and Public Policy with the University of Toronto. His research focuses on the privacy, security, and political implications of third-party access to telecommunications data. He can be contacted at chris@citizenlab.ca.

Introduction

New stories concerning serious security deficiencies in commonly used computer systems and networks are seemingly published every week. Such deficiencies have been exploited to spread malware designed to encrypt content so as to compel ransoms from the content's owners (Fruhlinger 2018), to facilitate the exfiltration of sensitive political data for information operations (Watson 2018; Hulcoop et al. 2017), to enable the deliberate destruction of data or physical computer systems (Snow 2016), and to enable the illicit harvesting of intellectual property for commercial gain (Brenner, Crescenzi Act 2006; Segal 2013). In each of the aforementioned types of security incidents, unauthorized actors took advantage of vulnerabilities in computer code by using malware that relied upon one or more computer exploits. An exploit is computer code which is written to take advantage of a computer system's vulnerability and subsequently cause the computer system to take an action in contravention of the desires of the computer system designer or operator. Exploit code is referred to as malware when it is used for malicious purposes, such as for the propagation of viruses, worms, trojan horse programs, ransomware, spyware, ransomware, adware, or scareware (Wilson et al. 2016, 6).

A range of Canadian government agencies exist to, in part, secure the public from digital threats like those just mentioned. The Canadian Cyber Incident Response Centre (CCIRC) was created to receive information about vulnerabilities as well as to communicate information about such threats to key stakeholders and the wider public. An element of the Communications Security Establishment's (CSE) mandate is to conduct information assurance operations, which include providing "advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada."(*National Defense Act* 1985)(s. 273.64 (1)(a)).[2] Furthermore, the Royal Canadian Mounted Police (RCMP) is responsible for identifying parties who exploit vulnerabilities contrary to law, and both investigate associated criminal activities as well as perform outreach concerning the need for businesses and individuals to stay safe when using digital systems.

Each of the aforementioned government agencies recognize that vulnerabilities can pose serious risks to public safety and the economy. However, the threat posed by the existence and exploitation of vulnerabilities are counterbalanced by Law Enforcement and Security Agencies' (LESAs) and Canada's foreign Signals Intelligence (SIGINT) agency's exploitation of vulnerabilities to carry out investigations and intelligence operations. The process by which

[2] As of the time of writing, the CCIRC and the information assurance elements of the CSE were being integrated into a common government entity, referred to as the Canadian Cybersecurity Centre. The Centre is expected to be operationally ready as of 2019.

Canadian government agencies counterbalance the need to protect citizens and businesses and government from exploitations of such vulnerabilities, and rely upon these same kinds of vulnerabilities to carry out their missions, remains masked in secrecy. The process of making evaluations about whether to disclose vulnerabilities to parties responsible for developing patches or, in contrast, retaining the vulnerabilities or exploits for state purposes are codified in policy frameworks referred to as 'Vulnerability Equities Processes' (VEPs). VEPs typically involve an interagency process to assess whether to disclose or retain vulnerabilities or exploit information. There is no indication that federal law enforcement agencies possess a VEP to determine when vulnerabilities are to be responsibly disclosed to vendors and software maintainers (Braga 2016) and Canada's SIGINT agency, the CSE, has declined to publish any details of its VEP (Braga 2017).

The balancing of interests -- between the protection of citizens and their systems and devices and ecosystems versus facilitating government agencies' abilities to intrusively act in the digital realm -- constitutes a question of political direction and prioritization of government activities. This balancing explicitly makes computer vulnerabilities, and the manners in which they might be disclosed or exploited, into political technologies insofar as they give rise to "arrangements of power and authority in human associations" (Winner 1988, 22). Specifically, the decision to focus on remediating vulnerabilities as a priority above making use of unpatched vulnerabilities constitutes a political decision of what affordances state agencies prefer: is the capability to potentially exploit a vulnerability to facilitate or advance an investigation or act of surveillance of higher importance than ensuring the given vulnerability is patched for all users so that they are protected from unauthorized parties taking advantage of the vulnerability, including criminals, hostile nation state operators, hacktivists, and state officials? And, moreover, in what ways should state agents who discover or learn about computer system vulnerabilities be kept accountable for their discovery, utilization, or disclosure of the vulnerabilities?

Reflecting on these questions and finding answers which maximize government accountability for government agencies' handling of computer vulnerabilities and exploits is of heightened importance given that the exploitation of vulnerabilities can enable government officials to deeply intrude into persons' private lives (Molnar, Parsons, and Zouave 2017; Bellovin et al. 2014). In the 1970s, the capability to deeply intrude into Canadians' private lives by way of live electronic surveillance (e.g. wiretaps) led to the development of an accountability regime which mandated judicial approval prior to using the live surveillance instruments, established detailed annual reporting requirements, and required notifying those targeted by the instruments (Parsons and Molnar 2018; Koutros and Demers 2013a; Canada Law Reform Commission of Canada 1986; Manning 1978). As will be argued in this paper, a publicly visible accountability regime is

needed to control the discovery, use, and disclosure of computer exploits by Canadian government actors for two reasons. First, because when utilized by Canadian state actors the vulnerabilities could be leveraged to deeply intrude into the private lives of citizens, and legislative precedent showcases that such intrusions should be carefully regulated. Second, because the vulnerabilities underlying any exploits could be discovered or used by a range of hostile actors to threaten Canadian citizens' and residents' of Canada personal security or the integrity of their democratic institutions. On these bases, it is of high importance that the government of Canada formally develop, publish, and act according to an accountability regime that would regulate state actors' use of computer vulnerabilities and exploits.

In making this argument, the paper proceeds in five parts. Part One discusses the current state of computer insecurity and why vulnerabilities are commonplace in computer systems and devices. It also explores the challenges associated with remediating such vulnerabilities. Part Two recounts the importance of governmental accountability before proceeding, in Part Three, to unpack the competing rationales for state agencies to disclose, or retain, knowledge pertaining to computer system vulnerabilities and exploits as well as the security issues linked to non-disclosure of such information. Part Four introduces the concept of citizen-focused security, which involves placing individual persons at the centre of a policy framework so as to better understand how, and why, it is important to develop an accountability framework paralleling this approach to security for electronic surveillance. Part Five, synthesizes the earlier parts to suggest that there may be overlapping, though unique, VEPs that apply to the acquisition and/or use of vulnerabilities for LESA and SIGINT operators. The article concludes by reemphasizing the importance of proactively developing a coherent and public VEP in Canada so as to guarantee governmental accountability for activities or decisions which have the potential to significantly intrude upon, or detrimentally affect, the private lives of citizens and residents of Canada.

1. The Insecurity of Contemporary Computing

Computer scientists and engineers are deeply challenged in developing computer systems and programs which lack vulnerabilities. These vulnerabilities are regularly exploited, and enable the commonplace occurrence of data breaches and exfiltration of data by unauthorized actors (Armerding 2018), the understandings that government law enforcement, security, and intelligence agencies have developed methods of gaining access to even the best-secured systems and devices (Armerding 2018; Wikileaks 2017; Shane, Perlroth, and Sanger 2017; Kerr 2017; Electronic Frontier Foundation 2016), and constant development and issuance of security patches to remediate vulnerabilities (See for example: Keizer 2018). Experts have warned in the past that any efforts to introduce additional weaknesses into already oft-insecure computer code —

including as part of irresponsible government encryption policies intended to gain access to the plain text of communications and stored data (Gill, Israel, and Parsons 2018) — will only worsen the already deeply problematic state of device and software (in)security (see: Schneier 2016; Abelson et al. 2015).

Indeed, as discussed by Herr and Schneier, "[d]esign insecurity is generally the result of poorly secured software, insecure programming languages, the growing complexity of commercial code bases, and simple human error, among a host of other causes." (Herr and Schneier 2017, 5). The effective complexity of contemporary computer systems and their interrelation with one another means that accidents in code will become 'normal' accidents insofar as such accidents "have a significant degree of incomprehensibility" associated with "the interaction of multiple failures that are not in direct operational sequence" (Perrow 2011, 23). The aim of most critical sectors is to try and mitigate and reduce the likelihood and regularity of such accidents (Perrow 2011).

One method of mitigating and reducing the likelihood of vulnerability-facilitated accidents is for security professionals to inspect and evaluate how software and systems perform and, where those inspections uncover irregularities in how the computer code operates, identify the root causes of such irregularities or vulnerabilities. Such professionals have a range of options for revealing what they learn. On the one hand, they may decide to not share the vulnerability and keep it secret for themselves (A. Wilson et al., 2016). This decision might be made because the researcher is engaging in their own intellectual development and has no desire to otherwise engage in a vulnerability remediation process or because of concerns that the organization to whom they reveal the vulnerability might become litigious or decline to patch the vulnerability, or because there is no one to whom to report the vulnerability, amongst other reasons. Alternately, the researcher might make the vulnerability public to all persons by publishing what is known about the weakness without prior notice to the vendor(s) or community which is responsible for the producing or supporting the vulnerable system or product, such as by posting a message to widely read mailing lists (Wilson et al. 2016). Researchers might opt for this approach on the basis that developers and maintainers of the affected software or systems may be more likely to remediate public vulnerabilities over those which are, in contrast, partially disclosed.

Partially disclosing vulnerabilities involves security researchers adhering to the ethics of 'responsible disclosure'. Responsible disclosure usually entails privately notifying the developer or maintainer of the system or software of the vulnerability, often with a working proof of concept code, with the intent of not publicizing the discovery until a software patch has been developed and issued (Maurushat 2014). However, responsible disclosure policies can be

complicated. First, companies or organizations producing or maintaining the systems or software in question may not have a public way of securely receiving vulnerability disclosures, thus inhibiting the ability for security researchers to inform the company about its vulnerabilities in a way that maintains the vulnerability's secrecy; revelation of the vulnerability, such as by communicating about it using unencrypted channels, increases the likelihood that the vulnerability might be obtained and exploited by another operator. Second, "...partial disclosure may be impossible when software has been "abandoned" by its original developers, or the original developer is unknown or has gone out of business, such that there is no obvious single party to disclose to" (Wilson et al. 2016, 11). Third, "[p]artial disclosure is also a risky option when attackers may already had discovered the vulnerability and begun exploiting it"(Wilson et al. 2016, 11).

In some cases, security researchers may be able to work through an intermediary to present the vulnerability to the organization responsible for the software or systems. A small handful of private organizations, such as HackerOne or the Electronic Frontier Foundation, work to facilitate such interactions. Alternately, researchers can disclose vulnerabilities and associated exploits to Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs). These teams engage in similar activities; they receive information pertaining to computer and system vulnerabilities and exploits and then work to coordinate the sharing of such information with parties which are competent or responsible for remediating the found problems (Dunn Cavelty 2014). CSIRTS and CERTs can operate under different authorities — they can have either regulatory or advisory powers (Morgus et al. 2015, 9) — but are generally mandated to "remediating and recovering" systems, whereas LESAs and SIGINT agencies who are informed of a security vulnerability and its exploitation may "focus on using the incident to gain more information in order to pursue the culprit or gather crucial intelligence, in lieu of remediating the damage." (Morgus et al. 2015, 14). Furthermore, should the CERT or CSIRT be regarded as being part of a country's intelligence community then researchers may be less inclined to disclose vulnerabilities or exploits to the organization(s) because they fear members of the intelligence community will utilize the discovered weaknesses instead of actively working to have them remediated (Morgus et al. 2015, 14).

Developing and making available a patch is only the beginning of the remediation process: "[f]or a patch to protect a system, it has to be applied. When the patch is not applied, the system is still vulnerable and can be exploited by myriad actors. Moreover, whether or not a company or entity chooses to patch immediately is a complex choice involving considerations of how best to maintain system functionality (and hence business operations) while improving computer security."(Pell and Finocchiaro 2017, 1588). The complexity of these choices are perhaps best

appreciated when considering the patching of Critical Information Infrastructure (CII); updates to CII may need to be custom crafted for the infrastructure or be impossible to develop because the vendor(s) which created the software or firmware for the CII no longer support the infrastructure in question (C. Wilson 2014, 125). And even when a patch is available for CII the costs of implementing it may be substantial. As discussed by C. Wilson (2014, 126):

> "... to install a software patch for a turbine generator on a regional power grid, the selected equipment must be stopped and taken out of service before the patch is installed. Stopping a power generator requires temporary redistribution of the electrical load throughout the grid, so that customer service remains uninterrupted as it is shifted over to substitute or backup turbine generators. Once the selected generator has been stopped, it must be allowed to cool down for several hours before it can be restarted with its new software security update installed. The process for shut-down, re-routing the electrical service load, and the final cool-down and turbine restart can potentially cost hundreds of thousands of dollars. In addition, the software security update must undergo a thorough set of testing to assure absolute reliability after installation and restart. CII facility managers and engineers will not accept a software update that may possibly malfunction, causing a service interruption for customers."

Moreover, in making a patch available other illicit operators may be able to determine how to take advantage of the (now patched) vulnerability: this can lead to at least two consequences. First, such operators may be able to 'weaponize' the vulnerability to target systems and software which have not yet implemented the patch. Second, illicit operators and benevolent security engineers alike may study the patch and subsequently identify new vulnerabilities that share common elements with the now-patched vulnerability.

Though specific rates are contested, vulnerabilities are often rediscovered by multiple parties. A RAND study found that 5.8% of some vulnerabilities were rediscovered (Ablon and Bogart 2017), whereas a report by Herr, Schneier, and Morris found that the rediscovery rate ranged from 10.8%-21.9% based on the software under examination and the severity of the vulnerabilities (2017). In other cases, nation state operators working within SIGINT agencies collect and use the undisclosed vulnerabilities of other, adversarial, state and non-state operators to provide a degree of ambiguity concerning which state is engaged in a given intelligence operation (National Security Agency 2008; 2010). While true that not all groups look for the same types or kinds of vulnerabilities — "[a]n intelligence organization is likely to have the engineering and mathematics capacity to take low-value or difficult-to-use vulnerabilities and combine them into a working exploit. Less capable groups may have to wait until they find a

vulnerability that can immediately be used to gain access to a computer system to develop a useful exploit" (Herr and Schneier 2017, 5) — the fact remains that "[e]very passing day brings a higher probability that someone else working to find vulnerabilities in the same piece of software will stumble upon the bug, leading to rediscovery." (Herr and Schneier 2017, 6). As just one concrete example of this, three separate teams of researchers discovered the same vulnerability in Intel chips during the same year, after the vulnerability had laid in wait for approximately twenty years (Greenberg, 2018b).

The potential for exploitation of vulnerabilities, and their (re)discovery by multiple classes of operators and researchers, may have serious implications for the security of information infrastructures. Consider a vulnerability in a popular piece of computer software such as the Microsoft Windows operating system. Such vulnerabilities might be used to target individuals en masse, in a non-targeted ransomware operation, to target specific high-value individuals in spear-phishing operations that leverage social information and computer weaknesses, or in deliberate state-backed operations meant to impact the operation of another state, such as by compromising electoral processes by corrupting voting machines or the systems which surround the actual act of voting (e.g. voter registries, email accounts of elected officials or campaign staff or electoral staff responsible for organizing and operating the election). Thus, the decision to disclose or retain a vulnerability in confident can be quite significant and have potentially far-reaching consequences. This decision may be particularly acute based on the sensitivity of the vulnerable system or device, the prevalence of the vulnerability across a range of operating environments (e.g. both critical and non-critical systems and infrastructure), the ability to effectively disseminate a patch, and the viability of patching systems before malicious operators realize how to develop and deploy exploits associated with the now-publicly patched vulnerability. With these decision points in mind, we now turn to the importance of government accountability processes, and how state actors might engage with these decision points and the consequences of such decisions in a way that ensures governmental actions are accountable to legislators and the public alike.

2. Accountability Gaps

Legislative assemblies have created numerous mechanisms to ensure that public officials and members of executive branches of government remain accountable to the citizenry. Such mechanisms often impose binding rules which are intended to delimit the powers and authorities of public officials. For any such mechanism to foster accountability, however, it must facilitate a particular relationship "where an individual or institution, and the performance of tasks or functions by that individual or institution, are subject to another's oversight, direction or request

that the individual or institution provide information justification for its actions."(Pelizzo and Stapenhurst 2013, 2). In effect, for accountability mechanisms to genuinely exist an institution or public person must be obligated to provide responses to a given series of questions concerning decisions or actions they have undertaken, and there be consequences should the party fail to render an account of their activities (Schedler 1999; Blick and Hedger 2008).

Political science often takes up accountability as a matter of hierarchies. In the Canadian context, Ministers are responsible to Parliament, and public officials are held to account within their given departmental structures. In both cases, actors are accountable to a larger or smaller forum which has the power to discipline inappropriate or undesired actions (Mulgan 1997; Anderson 2009).[3] For the purposes of this article, the concept of accountability is principally viewed through the lens of Ministers being formally accountable for the activities which are undertaken by their officials. Ministerial reporting is hierarchical, insofar as it occurs in formal contexts where an actor (the Minister) is responsible for responding to a forum (the legislative assembly), and is obligated to provide explanations or justifications for the actions which are conducted by the executive by way of the given department's authorities. The forum is empowered to receive this justification and, at least in theory, should be empowered to enact a sanction should the Minister fail to provide a meaningful account of their department's activities.

There can be at least two kinds of accountability failures in Parliamentary and other political systems, and which are tied to primary and secondary accountability gaps. Such gaps, generally, may arise when "reviewers or overseers do not have adequate powers or resources to match the conduct that is being reviewed" (Roach 2015, 169). Primary gaps arise when Ministers are not required per legislation to present specific information to the legislature and decline to provide such information when they are asked to provide the given information. In such situations the legislators are largely unable to specifically confirm that the Minister and their departments are behaving appropriately or within the law as written. A secondary gap, in contrast, arises "when legislative requirements compel a certain degree of government accountability but the required information is either not provided or there are insufficient resources or capacity to analyze the data in question" (Parsons and Molnar 2018, 149). Such gaps pose a threat to democratic

[3] This hierarchical conception of accountability has been expanded, arguably significantly, as a result of scholarly inquiry and now is sometimes understood as establishing unnecessary adversarial processes, as a concept needing to take on board how actors are sanctioned by their professional organizations, as addressing how institutions control official behaviours through internal organizational processes, as concerning how officials are accountable to the public directly and to legislators through parliamentary appearances, and how democratic dialogue disciplines institutions. As discussed elsewhere, "[t]hese changes to how accountability is conceptualized are based, in part, on the fact that private actors now assume roles and responsibilities that were carried out solely under the authority of state agencies" (Parsons and Molnar 2018, 147).

governance, especially when such gaps pertain to the government's ability to intrude into or disrupt a person's private life. If a gap exists such that legislators lack baseline information to subsequently hold the government to account, then legislators cannot ascertain whether the electorate's intentions and desires are being adequately adopted or represented by the government's choice of activities (Haggerty and Samatas 2010). Furthermore, should legislators be unable to represent their constituents' interests then cynicism can arise as citizens doubt the capabilities or competence of legislators in representing the citizenry's interests (Habermas 1998a, Parsons 2015). Finally, given that accountability regimes serve to ''help to ensure that the legitimacy of governance remains intact or is increased" by enabling Ministers to explain and justify their department's activities (Bovens 2007, 464), the absence of a strong accountability regime threatens to weaken the public's appreciation for rationales underlying controversial or non-controversial activities alike. Specifically, this justification process -- whereby citizens engage with their government and, as such, may see themselves in the laws and activities of their government -- is critical for law to be recognized as a legitimate expression of the citizens' and residents' own will. To put this another way, when governments do not fulfil their obligations to disclose information and enable the public's questioning of government activities and practices the democratic bonds between the public and their law and their government are diminished on the basis that as members of the public may feel that it is less likely that the government is undertaking activities which are both lawful and cohere with the public's democratic consent (Habermas 1998a, 1998b).

3. Competing State Interests and Vulnerabilities Equities Programs

Since between 2011 and 2014, public policy advocates, security researchers, government bureaucrats, and scholars have been debating whether, and under what conditions, governments should disclose vulnerabilities they learn about to the organizations or companies responsible for developing or maintaining the systems and software which are found to possess vulnerabilities. The question underlying this debate is summarized by Pell and Finocchiaro, when they write "...when a government agency discovers or purchases "zero-day" vulnerabilities, should it disclose them to relevant entities so that they can be patched, or should it retain them in continued secrecy to assist intelligence or law enforcement agencies with their lawful missions?"(Pell and Finocchiaro 2017, 1554). Such classes of vulnerabilities are those for which the manufacturer or system maintainer is ignorant of; there are no public defenses against discovered zero-day vulnerabilities until they have been disclosed or realized by the manufacturer or maintainer. As such, these vulnerabilities are often regarded as highly valued within the threat intelligence community, to the point that these vulnerabilities can be sold for

tens or hundreds of thousands of dollars per zero-day depending on their utility and the commonality of the affected software or systems (SpiderLabs Research 2016; Newman 2016; Osborne 2017).

Government agencies have utilized vulnerabilities to carry out their LESA- and SIGINT-related activities. The FBI employs Network Investigative Techniques (NITs) (Blake 2018) to, in part, investigate alleged illegal activities which occur online, and Canadian agencies have utilized general warrants to authorize their use of government malware and hacking since at least the mid-2000s (Personal conversation between author and Canadian government official, 2016). Moreover, Canadian provincial policing organizations have received product demonstrations of malware they could use for investigations (Braga 2015), though the costs are often significant and thus place such kinds of tools outside the realm of many forces (Personal conversation between author and former senior Ontario Provincial Police representative, 2017). No public data indicates that law enforcement agencies in Canada have a process to evaluate the equities which are in play when determining whether to use or report a vulnerability (Braga 2016). In contrast, reporting does indicate that the CSE possesses an equities process but details of that process are not public (Braga 2017).

In an era where computers are increasingly central to all elements of professional and private life, combined with efforts by private companies (Associated Press 2018) and public communities (Associated Press 2018; Internet Engineering Steering Group 2015) to improve the state of digital security (Kessler 2011), government investigative, security, and intelligence agencies all have reasons to acquire vulnerabilities that can be exploited to facilitate investigations and surveillance insofar as data security may be improving.[4] With such vulnerabilities in hand authorities can sometimes overcome cryptographic protections built to secure persons' data (Shane, Perlroth, and Sanger 2017; Kerr 2017; Electronic Frontier Foundation 2016; Gill, Israel, and Parsons 2018), intrude upon private communications that would otherwise be indecipherable (Shane, Perlroth, and Sanger 2017; Kerr 2017; Electronic Frontier Foundation 2016; see also: Gill, Israel, and Parsons 2018), compel devices to transmit information they wouldn't otherwise (National Security Agency 2007), cause devices to behave in self-destructive ways contrary to the desires of their operators (Zetter 2014; Snow 2016), or transit data around the global internet without other states necessarily knowing what is being transmitted or where it's going (National Security Agency 2016). In effect, these vulnerabilities

[4] It remains an unsolved question as to whether product and system security, in aggregate, genuinely is improving. Each week there are revelations of significant security failures even in some of the most 'secured' consumer products.

can be highly useful when adopted to fulfil government agencies' investigative or intelligence missions.

The capabilities to engage in the aforementioned activities come with the potential cost that other parties might discover, and make use of, the same vulnerabilities. Such discoveries can happen by co-incidental co-discovery of a vulnerability that can be exploited (Canada 2011; Herr and Schneier 2017), by an operator obtaining access to a LESA or SIGINT vulnerability after it has been deployed outside of the respective agency (Appelbaum et al. 2015b; Spiegel Staff 2013; Appelbaum et al. 2015a), or by a LESA or SIGINT (or private company servicing either class of agency) being breached and having their vulnerabilities exfiltrated and/or released to the public (Appelbaum et al. 2015b; Spiegel Staff 2013; Wikileaks 2017; Armerding 2017; Hay Newman 2018), amongst other methods. Sometimes these vulnerabilities are capable of causing significant global harm when used indiscriminately or without precise targeting by an operator; when the NSA's ETERNALBLUE Microsoft Windows malware was published by Russian operatives, the malware was subsequently used to cause at least $10 billion in damages (Greenburg 2018). This occurred despite the NSA alerting Microsoft to the vulnerability shortly following the Russian operator's threats to release malware, and Microsoft developing and issuing a patch for the vulnerabilities (Greenburg 2018), thus showcasing the limitations of remediating critical vulnerabilities.[5]

Government agencies should consider the political decisions being made when choosing to use, or to disclose, vulnerabilities or exploits pertaining to computer programs and systems given the potential for states to either independently discover vulnerabilities and develop malware capable of exploiting such vulnerabilities, the ability to purchase sophisticated malware from private companies to carry out operations, or the capacity to monitor security researchers' vulnerability discoveries and subsequently weaponize such vulnerabilities. The process of making such decisions is typically referred to as a Vulnerabilities Equities Process (VEP). VEPs, as of the time of writing, tend to be products of governments' executive branches as opposed to emerging from legislative assemblies' lawmaking processes. Executive-driven VEPs have the advantage of being updatable as thinking on how to weigh equities develops but, as creations of the executive, also risk being impermanent solutions to the problem of what government agencies should do upon discovering or acquiring exportable vulnerabilities (Fidler 2015, 450). Moreover, the

[5] In some cases, vulnerabilities that could lead to catastrophic harm have been secretly discussed and remediated, and only after a critical mass of systems operators have integrated and deployed the associated patches has the vulnerability in question been publicly disclosed. These kinds of situations can see governments, private organizations, and security professionals largely set aside digital communications out of fear that adversarial operators could learn of, and weaponize, such vulnerabilities. As an example, see: Joshua Davis. 2008. "Secret Geek A-Team Hacks Back, Defends Worldwide Web." *Wired*. November 24, 2008. https://www.wired.com/2008/11/ff-kaminsky/.

relative secrecy by which many executive branches of government operate means that VEPs might be quietly modified without the public or legislators knowing about, or understanding, the change(s) in policy.

The decision to report a vulnerability versus using it constitutes "a clash of competing social goods" which is what VEPs are meant to address (Bellovin et al. 2014, 47). If the primary concern of government agencies is "preventing the proliferation of exploits" then "society will be better protected by reporting the vulnerability early even if that risks the ability of the criminal investigation to conduct its authorized wiretap." (Bellovin et al. 2014, 47). In contrast, the "quest for geopolitical power and a strategic military advantage over another state's cyber defences is sometimes at odds with the state's responsibility to ensure public safety and secure cyberspace, because developing new exploits or leaving old vulnerabilities unaddressed creates risk in the system" (Bradshaw 2015, 14). A VEP is intended to address this contrasting set of responsibilities.

To be sure, there may be a range of different *kinds* of vulnerabilities and a VEP might lead to some being disclosed and others retained and kept secret by government agencies. Highly capable governments agencies, such as Western SIGINT agencies, might enjoy engineering and mathematics competence that exceeds that of most parties, such that they can create entirely novel kinds of malware and undertake what are, at the time, regarded as boldly novel operations (Herr and Schneier 2017, 5). The Stuxnet operation, where Israeli and USA operators developed and deployed malware to damage Iranian nuclear centrifuges, is an example of such a novel operation given the string of vulnerabilities which were used and targeted at highly protected elements of the Iranian government's critical infrastructure (Zetter 2014). In other cases, government agencies might licence access to malware tools that the agencies themselves are not competent to develop; companies such as Hacking Team (Zetter 2014; Marczak, Scott-Railton, and McKune 2015), NSO Group (Zetter 2014; Marczak, Scott-Railton, and McKune 2015; Marczak and Scott-Railton 2016) and Gamma Group (Marquis-Boire et al. 2013) have all offered relatively sophisticated products designed to facilitate LESA and SIGINT operations, often by countries' federal and state agencies which are largely non-compliant with international human rights law or principles (Amnesty Staff 2018; see also: Shezaf and Jacobson 2018).

By the same merit, government agencies in Canada and the USA routinely assert that they do, in fact, disclose the majority of the vulnerabilities which they discover or learn about (Braga 2017; Pell and Finocchiaro 2017). However, such assertions are not auditable by non-members of the executive nor are there required reporting formats which the executive in either country is required to adhere to. Given that "...a significant overarching goal of any workable VEP should

be to provide meaningful government accountability and transparency without unduly burdening legitimate offensive operations and lawful investigations" (Pell and Finocchiaro 2017, 1558), any VEP must directly engage with sensitive political questions and issues associated with social order and the terms upon which it is appropriate to intrude upon, and interfere with, the private seclusion of individuals or private organizations inside and outside of a sovereign state.[6] A VEP needs to be suitably clear so as to hold the government to account: this means that data concerning policies, as a bare minimum, must be public and that there be a mechanism through which to hold the government to account for its policy positions and its keeping in bounds of such positions. To make clear the implications of deciding to retain a vulnerability, I have previously argued that:

> … [b]y concealing the weakness of the device or exploit code used to perform the [Computer Network Operation], not only is the security of a specific target compromised, but so is the security of all other persons who happen to use the same device or rely on the same codes. Exploits are reproducible, and so the failure to disclose vulnerabilities can mean that other parties (e.g. nation-state actors, cyber mercenary firms, independent hackers, or academics) can also identify and exploit the same vulnerabilities. Furthermore, in failing to notify companies of weaknesses in their defenses or flaws in their software code those companies can suddenly fall victim to the state's exploit code when it is accidentally released to the public. (Molnar, Parsons, and Zouave 2017, 8)

In effect, the decision to retain a vulnerability may have substantial impacts on both the persons for whom the state is acting on behalf of -- the citizens and residents of the given state -- as well as persons who are external to the state -- that is, persons who are citizens and residents of different states. The commonality of the devices, software, and systems which persons around the world use mean that any vulnerabilities in commonly-used technologies have the potential to have impacts upon any and all persons around the world. Furthermore, while members of one state -- such as Canada -- might approve of the government of Canada retaining vulnerabilities that could be used to intrude into the networks of adversarial states, normative positions whereby states hoard exploitable vulnerabilities to engage in espionage or investigations or combat give rise to the possibility that other states will mimic this position. Should states generally adopt a 'stockpile-the-vulnerabilities' policy position, then all citizens, around the globe, would be less likely to be able to use maximally secure systems as private companies find and sell

---

[6] Though outside the scope of this paper, the acquisition or discovery of vulnerabilities with an aim of utilizing exploits to deliver malware is also a key component of states' digitally-mediated cyberware capabilities. As such, there are also military-related equities that may sometimes be included in a responsible VEP policy. However, the state of military acquisition of vulnerabilities has been set aside for the purposes of avoiding a discussion of the unsettled law of war that pertains to digitally-mediated cyberconflict.

vulnerabilities and nation-state actors refuse to 'disarm' based on a fear that other states will refuse to disclose vulnerabilities that they themselves find or obtain.

4. Citizen-Focused Security and Vulnerability Accountability

The Internet has long-been characterized as a network of networks, where individuals work collectively to develop and improve and secure its characteristics (Mueller 2010; DeNardis 2014; Deibert 2013). The act of collectivist development and maintenance is demonstrated by the multi-stakeholder formats which are routinely used, and advocated for, when major decisions pertaining to the global Internet are being made (Mueller 2010; DeNardis 2011). This kind of stewardship "...is an old idea. Historically, Internet stewardship has referred largely to strengthening the technical aspect of internet operation and governance. On this view of stewardship, the ease of communication and access to information engendered by the Internet embody a global public good, which states should nurture"(Peter Margulies and Margulies 2017, 464).

States have increasingly adopted a view of the Internet as a zone wherein criminal or other illicit activities take place, as well as important for commercial activities and facilitating state practices (Department of Defence 2018; United States Government 2018; Canada 2018, 2016). With regards to the former positions, Western nation-states increasingly have 'cyberforces' associated with their militaries (Strobel 2018; Braga 2017; Parsons et al. 2017a, 2017b), seek out vulnerabilities to use in domestic and international activities (Bellovin et al. 2014; Electronic Frontier Foundation 2016; Gjelten 2013; Communications Security Establishment Canada 2009/2010, Cox 2016), and acquire malware from private companies to take advantage of vulnerabilities in popularly used devices[7] and software.[8]

In all cases, these acquisitions of vulnerabilities, exploit code, and malware are meant to enable to state to protect against threats to national security. As discussed by Dunn Cavelty, such threats are "...presented as possible disruption to a specific way of life -- one building on information technologies, economic performance and "critical" functions of infrastructures -- but the direct threat to human security, especially a threat that undermines acquired values such as anonymity, privacy, freedom of speech, free access to information, etc. does not figure prominently in the

[7] See: https://www.elcomsoft.com/eift.html

[8] Such companies can include, but are not restricted to, Gamma Group (FinFisher), Hacking Team (Galileo), and NSO Group (Pegasus).

policy discourse." (Dunn Cavelty 2014, 704). In effect, the framing and rationale for the acquisition of exploits to develop malware for state operations is state-centric, as opposed to designed first and foremost to foster the rights and freedoms of denizens of the Internet or of citizens and residents of sovereign states. A concept of citizen-focused security and vulnerability disclosure, then, would be necessarily oriented first and foremost to account for the common good -- which has historically been undertaken in multi-stakeholder models of governance for Internet systems -- and would avoid actions that threaten to undermine the privacy, security, or basic rights of citizens and residents of states.

To facilitate the realization of basic rights, democratic states must at a minimum integrate regimes of public accountability when undertaking actions that have the potential to affect or threaten the well-being of their own citizens and residents, as well as other nations' citizens and residents who may be developing interconnected systems upon which members of the state depend on. In other words, while a citizen-centric approach to security entails establishing a legal obligation to develop accountability regimes to facilitate trust in government and legitimize government activities that are undertaken on behalf of a state's own citizens and residents, there should also be a normative and practical accountability in government practices that affect citizens and residents of other nations. This latter line of accountability, as it pertains to the development or acquisition and subsequent use or disclosure of computer code vulnerabilities or exploits, is not intended to accomplish the same goals as traditional 'hierarchical' forms accountability. Rather, in rendering government practices transparent and accountable, foreign citizens and residents can be assured that they can safely adopt and use digital tools and systems which are, themselves, used to create products for the state's own citizens as well as to interconnect with the same devices, systems, and software used by the state and its citizens. The interdependency of systems and devices, in effect, is predicated on a mutual belief that other members of the network are not intentionally acting in a malicious manner; while, of course, criminal actors may behave in such a manner, should states behave similarly then the baseline presumption that the Internet and its connected systems constitute a commons that must be collectively stewarded are threatened, to the effect of undermining the norms which have led to the Internet becoming what it is and driving significantly new ways to engage and express basic rights, along with the economic and social benefits oft-attributed to Internet-connected systems and software.

There may, however, be cases where some government-regulated vulnerabilities are relied upon to accomplish certain state functions that involve intruding into computer systems and networks. What is essential is that such code and its operation is carefully accounted for in a public manner, so as to retain trust between the stakeholders of Internet-connected systems and devices.

Historically, governments in Canada and the United States, along with other Western governments, developed reporting structures to explain when they used exception means to intrude into private life (Parsons and Molnar 2018). A citizen-centric approach to developing a VEP might, as an example, indicate the regularity at which certain government agencies have received or discovered exploitable vulnerabilities, as well as whether they reported or used such information. Moreover, a citizen-centric VEP might be deliberately and explicitly biased towards establishing conditions upon which vulnerability information is disclosed to vendors or maintainers of software, devices, and systems. To be clear: what is being argued for is that a citizen-centric approach to security, as associated with VEP, would entail states adopting a defensive-first approach to cybersecurity which is biased towards disclosing discovered vulnerabilities and exploits, and retaining only a small subset for offensive operations which may be required to conduct state functions. And, as will be discussed below, even those retained vulnerabilities and exploits might need to be disclosed upon their use in certain enumerated situations.

If a citizen-centric concept of security involves facilitating the basic rights of citizens and residents of sovereign states, first, as opposed to prioritizing the security of the state itself and its critical infrastructures, then accountability is essential as an element of such citizen-centric security. This essentiality follows from accountability enabling citizens to realize the extent(s) to which their basic rights are being protected *or* threatened by their governments. Should accountability reporting reveal that a given government was deliberately acquiring and not disclosing a significant number of exploitable vulnerabilities, then citizens may question whether the retention of such security vulnerabilities are reflective of the given government's deprioritization of secure modes of communication which are designed to foster freedoms of association and speech and religion, as an example. Similarly, should reporting reveal that governments are in fact disclosing vulnerabilities in order to secure systems essential in the digital age for the exercise of basic rights, then citizens and residents might be relieved to know that the government has highly focused on the protection of their basic rights, even when doing so may make certain law enforcement and security investigations more challenging, and stymie certain kinds of foreign signals intelligence operations.

5. Applying Citizen-Focused Accountability Security to Government Acquisition and Use of Vulnerabilities

Canadian government agencies might adopt a range of VEPs that share some commonalities but which are not uniform in their character. In this section I briefly address the potential impacts that accountability reporting might have on the use of exploitable vulnerabilities for law

enforcement, for security services, and for foreign signals intelligence agencies. Next, I address the question of whether such reporting and accountability rules out the usage of vulnerabilities by government agencies. I conclude by outlining some basic minimum policies which might be adopted to facilitate citizen-focused security practices and the importance of adopting such practices to protect citizens' and residents' of Canada's basic rights and core democratic institutions.

The effects of reporting of government surveillance operations will, presumably, vary based on the kind(s) of agencies which are involved in the reporting. Law enforcement agencies are already accustomed to having to comply with reporting requirements when they engage in live electronic surveillance using telephonic, audio, or visual surveillance (Parsons and Molnar 2018; Koutros and Demers 2013b). Many of the categories for those reports -- such as number of warrants sought and obtained to conduct surveillance, efficacy of the surveillance insofar as it produces evidence used in court and in securing convictions, and denoting the kinds of criminal activities which are investigated using these kinds of surveillance -- can be directly carried over, though additional reporting fields would presumably also need to be included. As an example, law enforcement agencies' reports might need to include a clearly stated set of conditions wherein the agency or department would disclose or retain a vulnerability which was either procured or acquired or discovered. Reports could also, presumably, indicate when vulnerabilities had been disclosed following the introduction of evidence attributed to the vulnerabilities in court, following the open courts principle.

In the case of security agencies, such as the CSIS, security considerations may mean that reporting is less granular; while the specific number of vulnerabilities which were disclosed below a certain number might be presented in reports in bands, above a certain threshold more granular numbers might be included in reporting of how many vulnerabilities had been discovered/acquired and disclosed. For greater certainty, and as an example, this might mean that when fewer than 100 vulnerabilities were discovered or acquired, a band of 1-99 is used for accountability reporting, whereas when 100 or more vulnerabilities were acquired or disclosed then more specific numbers might be adopted, either in a band format (e.g. 100-125) or specific number (e.g. 117). Such security considerations could apply on the basis that foreign adversaries might interpret the number of vulnerabilities identified/disclosed as indicative of relative capabilities and, as such, some restrictions on the information pertaining to security service work may be appropriate to facilitate national security investigations meant to suppress efforts to interfere with Canadians' and residents of Canada's basic rights (e.g. rights to vote, to communicate, to practice their religion, etc).

Foreign signals intelligence agencies, also, might be rendered more accountable by requiring them to account for their collection, use, and disclosure of vulnerabilities and exploits. Such accountability might be enforced through at least two mechanisms. First, the Centre for Cybersecurity is integrating key elements of the CSE's information assurance directorate, as well as elements of Canada's national CERT, the CCIRC. CSE might disclose some of its information pertaining to vulnerabilities to the Centre and the Centre, in turn, might subsequently publicly report on the regularity at which vulnerabilities are being reported to it and which are then disclosed to vendors or systems developers. Not all vulnerabilities may be disclosed, however, on the basis that a small subset are needed to fulfil a de minimis offensive mission associated with the CSE. The retention and use of such vulnerabilities may constitute a sufficiently significant national secret that information about such activities cannot be productively declassified for the general public. In such a case, the CSE could avail itself of its review body -- the National Security Intelligence Review Agency (NSIRA)[9] -- as well as the committee of parliamentarians -- the National Security and Intelligence Committee of Parliamentarians (NSICOP)[10] -- which are tasked with working from within the executive to evaluate the activities undertaken in the course of Canadian national security activities.

The purpose of accountability reporting is not to stop government agencies from acquiring and utilizing vulnerabilities or exploits in the course of accomplishing their respective missions. However, restrictions are appropriate given the different resources associated with given state actors and their competing investigative/intelligence and protective cybersecurity missions. In the case of law enforcement, as an example, it may be the case that any vulnerabilities these agencies discover are expected to be automatically disclosed. This disclosure should not be understood as preventing the use of government-authorized malware operations; even after vendors have issued patches to remediate vulnerabilities, those vulnerabilities often linger for extensive periods of time (see: Verizon 2016; Shepardson 2016). Moreover, if LEAs are required to only exploit known-patched vulnerabilities then these agencies may actually reduce the costs of investigations insofar as retroactively determining how to exploit a found vulnerability tends

---

[9] The NSIRA is designed to ensure that Canada's national security agencies are complying with the law and that their actions are reasonable and necessary. The Agency's findings and recommendations are to be provided to relevant Ministers through classified reports. NSIRA is also expected to produce an unclassified annual report to Parliament summarizing the findings and recommendations provided to Ministers.

[10] The NSICOP is a statutory committee of parliamentarians appointed by and administratively housed within the executive branch. The committee would have a broad government-wide mandate to scrutinize any national security matter. The NSICOP is empowered to perform reviews of national security and intelligence activities including ongoing operations, and strategic and systematic reviews of the legislative, regulatory, policy, expenditure and administrative frameworks under which these activities are conducted. It may also conduct reviews of matters referred by a minister. Given its broad mandate to review any operation, which includes ongoing operations, a minister has the authority to stop such a review if it would be injurious to national security.

to be easier and more affordable as compared to discovering the relevant exploitable vulnerability for the first time and with no clues as to its existence. In situations where LEAs absolutely require a novel mode of accessing data from a service, piece of software, or a device then they could make a formal (and auditable) request to either the domestic security service or foreign SIGINT agency for assistance.

Security services may require a slightly broader policy framework to determine when, and if, vulnerabilities should be disclosed. Generally, where a vulnerability is associated with network infrastructures as opposed to end-point devices, the vulnerabilities should be deeply biased towards disclosure -- and perhaps even mandated so -- on the basis that leaving such vulnerabilities unpatched runs the risk of facilitating catastrophic attacks on critical infrastructure (Bellovin et al 2014; Landau 2010) and consequently endanger national security. This may mitigate some of the potentials to engage in surveillance of valid security service targets but, by the same light, will ensure that critical national infrastructures are not targeted or taken advantage of by hostile operators working contrary to Canada's national interests. Furthermore, while intrusions into end-point devices (e.g. mobile phones, personal computers, automobiles, fitness trackers, etc) can be deeply revealing of personal life and thus threaten the exercise of basic rights, a presumptive difficulty of engaging in such operations along with the risk of discoverability of such end-point operations and legal restrictions on targeting, should restrict the actual willingness of agencies to conduct such operations. And, should the CSIS' end-point vulnerabilities be discovered as being used by other operators -- such as by the CSE as it monitors foreign operators' activities or by other friendly security or intelligence services -- the CSIS could then automatically move towards disclosing the vulnerability and remediate the risks linked with the vulnerability's usage.

The most challenging party to integrate into a VEP is perhaps a foreign signals agency; such agencies thrive by both targeting endpoints with known and previously-unknown vulnerabilities, as well as by targeting networking appliances responsible for carrying large volumes of data traffic. Again, there should be a strong bias towards disclosing found vulnerabilities in networking infrastructures with the caveat that, where those infrastructures are largely not present in Canada or the infrastructures of its closest allies, there may be greater leeway in delaying disclosure. As an example, where a networking company is largely or entirely banned from selling equipment into Canada and to Canadian networking infrastructures (as well as those of close allies), then retaining and utilizing vulnerabilities associated with such a company might be more appropriate than retaining and utilizing vulnerabilities for devices which are used by legitimate foreign intelligence targets *as well as* Canadian companies and government agencies and those with whom Canada has a close strategic relationship.

In all cases, should an agency decline to disclose a vulnerability when it is first discovered there should be repeated re-evaluations of that decision. Further, the decision to disclose, or not disclose, cannot be made purely by the law enforcement, security, or foreign intelligence agencies. As noted by Pell and Finocchiaro, the role of determining if a vulnerability should be disclosed should not "...be the job of that individual investigator, or left solely to the discretion of the FBI or other law enforcement agency ... There are significant competing equities at stake that demand analysis and review -- not only those of the "users" who exploit a vulnerability (which may be more than one entity exploiting or planning to exploit a specific vulnerability), but also those of the agencies in the [United States Government] who focus on network defense and information assurance." (Pell and Finocchiaro 2017, 1584). In the Canadian context, potential government parties which should be involved in a VEP include Innovations, Science and Economic Development, Government Affairs Canada, Office of the Privacy Commissioner of Canada, Royal Canadian Mounted Police, Canadian Border Services Agency, Communications Security Establishment, Canadian Security Intelligence Service, Elections Canada, Treasury Board Secretariat, and Canadian Revenue Agency, at a minimum. Furthermore, members of civil society should be included in any such deliberations, perhaps subject to obtaining appropriate security and secrecy clearances, so that the public's position is clearly expressed. Similarly, some members of private industry *or* members of organizations representing private industry ought to be involved so as to bring non-government perspectives into the decision-making process. It is important that civil society and private companies not merely be brought in to offer opinions but are truly, and fully, made to be part of decision-making so as to lend legitimacy to a process which otherwise runs the risk of being perceived as an opaque and self-justificatory policy. To ensure that neither private corporations nor civil society are used to merely justify government activities, some mode of reporting on the regularity at which there were dissents on whether to disclose a vulnerability are important to make public in perhaps a generalized sense and, in a more specific sense, to security-cleared bodies such as the NSIRA and NSICOP.

Efforts to prioritize the discovery, and remediation, of vulnerabilities serves a citizen-focused approach to security insofar as closing vulnerabilities reduces the likelihood that basic rights might be intruded upon, or violated, by operators exploiting those vulnerabilities. What is key to this citizen-focused approach is that government agencies not prioritize short-term gains -- the abilities to exploit hither unknown vulnerabilities -- at the expense of generating long-term harms -- the insecurity of citizens and residents of Canada, and parties with whom Canada engages with -- or at the cost of promulgating citizen-hostile security norms -- which are associated with states identifying, collecting, and stockpiling vulnerabilities.

Finally, efforts to remediate vulnerabilities are important to prioritize to secure particular institutions which are essential in facilitating or protecting citizens and residents' basic rights. As was revealed in electoral processes in the United States of America in the 2016 presidential elections, vulnerabilities can be exploited by hostile operators to interfere in party-based and government-based organizations that are critical to elections. Remediating vulnerabilities can reduce the attack surfaces that operators can take advantage of by, for example, limiting the abilities of hostile operators to enter communications systems and subsequently exfiltrating staff members' and candidates' private communications. In the absence of aggressive efforts to disclose vulnerabilities and thus delimit attack surfaces, candidates and their staff may limit their own communications to the effect of running less engaging or intellectually intensive campaigns, with the effect of presenting less representative campaigns to citizens who are evaluating for whom they should vote. Moreover, by disclosing vulnerabilities -- and having them patched by institutions responsible for running elections and electoral infrastructures -- the electorate's trust in the electoral system may be better maintained. Even where the exploitations of a vulnerability does not lead to a material change in electoral outcomes, such as flipped votes or removal of persons from voter registries, the very fact that electoral systems have been compromised may detrimentally affect the citizenry's perception of the legitimacy of the election. This perception, in and of itself, can arguably be as (or perhaps more) damaging to the legitimacy of an elections. As such, strong biases towards disclosing vulnerabilities by all government agencies can serve to reduce the attack surfaces presented to hostile operators and, thus, have indirect or direct consequences for maintaining the actual and perceived legitimacy of electoral processes, as well as in the parties and institutions involved in such processes.

6. Conclusion

This article has argued that a human-centric approach to security demands that a vulnerabilities equities process, which involves a high degree of reporting accountability, be established in countries such as Canada where government agencies are actively involved in obtaining and exploiting vulnerabilities in furtherance of their investigative, security, and intelligence missions. Such accountability is required to ensure that Canadian agencies are being properly regulated in their intrusion into Canadians' private life, as well as to engender and maintain Canadians' trust in the integrity of their democratic institutions. Critically, such reporting will ensure that primary accountability gaps — which are prompted by a lack of a legislative requirement for Ministers to present specific information to the legislature and decline to do so when they are asked to provide the given information — would be obviated, leaving only the risk of secondary gaps that result from legislative assemblies either lacking the resources to analyze the provided materials

or sanction the relevant Minister for presenting insufficient information in the publicized reporting.

The requirements that government agencies prepare, and publicly present, accountability reports concerning their acquisition, use, and disclosure of vulnerabilities would not preclude the government from using malware to accomplish legitimate missions. However, the reporting would enable legislators and the public alike to verify government assertions that most vulnerabilities are disclosed, and that the exploitation of such vulnerabilities by law enforcement and security agencies are relatively rare occurrences. Where national security sensitivities limit the degree of detail that agencies could publicly report then government national security review infrastructures — found in NSIRA and NSICOP — along with a robust VEP process that includes members of civil society and private business could served to verify that government statements accord with the realities of how vulnerabilities and exploits are dealt with by government agencies.

Government agencies that are most likely to exploit vulnerabilities in the service of their investigative or intelligence missions are, also, the institutions which are responsible for mitigating threats and harms to national interests. For these agencies to adopt a more human-centric approach to security they may need to modify what is emphasized in the protection of national security interests. Specifically, while existing policies emphasize the importance of critical infrastructure, key sectors of the economy, and government functions, they rarely focus on national security as critically linked with citizens' and residents' basic rights. Turning to focus, first and foremost, on the securing and protecting and facilitating of such rights may shift the attention to increasingly defensive and protective measures. Such measures would be designed to ensure that citizens and residents do not avoid certain digitally-mediated activities out of fear that their communications or other activities were susceptible to hostile operators, be they criminal in nature, foreign intelligence and security operators, or even domestic law enforcement and security services that may have a history of infringing on the rights and freedoms of law-abiding persons who are engaged in risky or abnormal (yet lawful) activities. Furthermore, in focusing on basic rights as the driver for vulnerability assessments certain vulnerabilities in systems and software — such as those used to enable the justice or electoral systems — might be recognized as having an overwhelming 'vote' in an equities process, whereas such 'votes' might be less overwhelming in the absence of a human-centric approach to cybersecurity.

To be sure, considerable work and research surrounding government discovery of computer exploits remains to be done. Interviews with elite stakeholders might better reveal the process of

vulnerabilities equities processes and some of the ways in which the equities process is currently structured, and the rationales for such structurations. It remains unclear just how unique VEPs are across government agencies and such interviews might cast some light on the exact nature of existent VEPs, with the ultimate goal of evaluating the extent to which they promote offensive or defensive cybersecurity policies. More detailed analysis of what should be in VEP reports is also needed; while this article has sketched some fields of data to be recorded, and suggested the importance of banding some data in order to protect national security information, much remains to be done before scholars and policymakers can better understand the potentials and limitations of such reporting. Finally, though this article has begun to discuss the link between basic rights, accountability, and human-centric security policies, more should be done to fully unpack the distinctions between human-centric versus institutional-centric policies and map the outcomes of such distinctions, as well as forecast the mid-term implications of continuing to rely on institutional-centric approaches when developing and weighing equities in VEP policies. While the unearthing of current policies and proposals of next-generation policies are made more complicated by the national security and public policing dimensions of the topic of vulnerability discovery and exploitation, VEP policies are of critical importance to develop and publish given the intrusive capabilities of state uses of malware. Just as the liberal state has carefully established conditions to delimit the use of live electronic surveillance such as wiretaps, it — and we — must develop a correlate set of conditions to restrict and regulate the state's intrusion into our digital private lives using what is arguably an even more intrusive investigative and intelligence capability.

Bibliography

Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Landau, Susan; Neumann, Peter G.; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael A.; and Daniel J. Weitzer. 2015. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." Journal of Cybersecurity 0(0).

Ablon, Lillian, and Andy Bogart. 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits.

Allodi, Luca. 2015. "The Heavy Tails of Vulnerability Exploitation." In *Lecture Notes in Computer Science*, 133–48.

Amnesty Staff. 2018. "Amnesty International Among Targets of NSO-Powered Campaign." Amnesty International. https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/.

Anderson, Jonathan. 2009. ‘‘Illusions of Accountability: Credit and Blame Sensemaking in

Public Administration." *Administrative Theory & Praxis* 31(3).

Appelbaum, Jacob, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt, and Michael Sontheimer. 2015a. "NSA Preps America for Future Battle." *Der Spiegel*, January 17, 2015. http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409-2.html.

———. 2015b. "The Digital Arms Race: NSA Preps America for Future Battle - SPIEGEL ONLINE - International." SPIEGEL ONLINE. SPIEGEL ONLINE. January 17, 2015. http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

Armerding, Taylor. 2017. "Shadow Brokers Cause Ongoing Headache for NSA." *Naked Security*, November 15, 2017. https://nakedsecurity.sophos.com/2017/11/15/shadow-brokers-cause-ongoing-headache-for-nsa/.

———. 2018. "The 17 Biggest Data Breaches of the 21st Century." *CSO*, January 26, 2018. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure." *Information Systems Research* 21 (1): 115–32.

Associated Press. 2018. "Apple to Close iPhone Security Gap Police Use to Collect Evidence." *The Guardian*, June 14, 2018. https://www.theguardian.com/technology/2018/jun/14/apple-close-iphone-security-gap-police-fbi-collect-evidence.

Baud, Patrick F. n.d. "The Reform of National Security Accountability in Canada." *Canadian Human Rights Yearbook = Annuaire Canadien Des Droits de La Personne*.

Bellovin, Steven M., Matt Blaze, Sandy Clark, and Susan Landau. 2014. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet." *Northwestern Journal of Technology and Intellectual Property* 12 (1).

Blake, Andrew. 2018. "Appeals court OKs evidence collected by FBI malware during child-porn sting." *The Washington Times*, January 27, 2018. https://www.washingtontimes.com/news/2018/jan/27/appeals-court-oks-evidence-collected-fbi-malware-d/.

Blick, Andrew, and Edward Hedger. 2008. "Literature Review of Factors Contributing to Commonwealth Public Accounts Committees Effectively Holding Government to Account for the Use of Public Resources." Overseas Development Institute.

Bovens, Mark. 2007. "Analyzing and Assessing Accountability: A Conceptual Framework." *European Law Journal* 13(4).

Bradshaw, Samantha. 2015. "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity." 23. Global Commission on Internet Governance.

Braga, Mathew. 2015. "Canadian Police Looked Into Buying Hacking Software." *Motherboard*, July 7, 2015. https://motherboard.vice.com/en_us/article/3dkmyv/canadian-police-looked-into-buying-hacking-software.

———. (2016) 2016. "What Happens When Canadian Cops Find a Software Security Flaw?" *Motherboard*, 2016. https://motherboard.vice.com/en_us/article/78kkze/what-happens-when-canadian-cops-finds-a-software-security-flaw.

———. (2017) 2017. “When Do Canadian Spies Disclose the Software Flaws They Find? There’s a Policy, but Few Details.” *CBC News*, 2017. https://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007.

———. 2017. “How, When and Where Can Canada’s Digital Spies Hack? Government Makes Some Suggestions in CSE Act.” *CBC News*, June 20, 2017. https://www.cbc.ca/news/technology/bill-c59-cse-act-spies-canada-hacking-foreign-cyber-ops-1.4169689.

Buchanan, Ben. 2016. “The Life Cycles of Cyber Threats.” *Survival* 58 (1): 39–58.

Canada Law Reform Commission of Canada. 1986. “Electronic Surveillance.” Working Paper No. 47.

Canada, Public Safety. 2011. “Implementing PHP cURL Verifypeer Option in Applications Requiring SSL Certificate Verification.” Public Safety Canada. December 20, 2011. https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2011/in11-003-en.aspx.

———. 2016. “Our Security, Our Rights: National Security Green Paper, 2016 (Background Document).” Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf.

———. 2018. “National Cyber Security Strategy: Canada’s Vision for Security and Prosperity in the Digital Age.” Government of Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.

Canfield, Casey, Frankie Catota, and Nirajan Rajkarnikar. 2015. “A National Cyber Bug Broker: Retrofitting Transparency.”

Coles-Kemp, Lizzie, Debi Ashenden, and Kieron O’Hara. 2018. “Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen.” *Politics and Governance* 6 (2): 41–48.

Communications Security Establishment Canada. 2009/2010. “CSEC Cyber Threat Capabilities: SIGINT and ITS: An End-to-End Approach.” https://assets.documentcloud.org/documents/1690224/doc-6-cyber-threat-capabilities.pdf.

Cox, Joseph. 2016. “The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a Thousand Computers.” *Motherboard*, January 5, 2016. https://motherboard.vice.com/en_us/article/qkj8vv/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace*. Signal.

DeNardis, Laura. 2011. *Opening Standards: The Global Politics of Interoperability*. MIT Press.

———. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

Department of Defence. 2018. “Summary: Department of Defense Cyber Strategy.” United States Government. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Dunn Cavelty, Myriam. 2014. “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.” *Science and Engineering Ethics* 20 (3): 701–15.

Electronic Frontier Foundation. 2016. “The Playpen Cases: Frequently Asked Questions.” Electronic Frontier Foundation. 2016. https://www.eff.org/pages/playpen-cases-frequently-asked-questions.

Fidler, Marilyn. 2015. “Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis.” *I/S: A Journal of Law and Policy for the Information Age* 11 (2): 405.

Fox, Jonathan. 2007. “The Uncertain Relationship between Transparency and Accountability.”

Development in Practice 17 (4-5): 663–71.

Fruhlinger, Josh. 2018. "What Is WannaCry Ransomware, How Does It Infect, and Who Was Responsible?" *CSO*, August 30, 2018. https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html.

Gill, Lex, Tamir Israel, and Christopher Parsons. 2018. "Shining a Light on the Encryption Debate: A Canadian Field Guide." Citizen Lab.

Gjelten, Tom. 2013. "First Strike: US Cyber Warriors Seize the Offensive." *World Affairs* 175 (5): 33–43.

Greenburg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired*, July 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greenberg, Andy. 2018b. "Triple Meltdown: How so many researchers found a 20-year-old chip flaw at the same time." *Wired*. January 7, 2018. https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/

Habermas, Jürgen. 1998a. ''On the Internal Relation between the Rule of Law and Democracy." In Jürgen Habermas, ed., *The Inclusion of the Other: Studies in Political Theory*. Cambridge: The MIT Press.

Habermas, Jürgen. 1998b. ''Three Normative Models of Democracy." In Jürgen Habermas, ed., *The Inclusion of the Other: Studies in Political Theory*. Cambridge: The MIT Press.

Haggerty, Kevin D. and Mina Samatas. 2010. ''Introduction: Surveillance and Democracy: An Unsettled Relationship." In Kevin D. Haggerty & Minas Samatas, eds., *Surveillance and Democracy*. Canada: Routledge-Cavendish.

Hay Newman, Lily. 2018. "The Leaked NSA Spy Tool That Hacked The World." *Wired*, June 3, 2018. https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/.

Herr, Trey, and Eric Armbrust. 2015. "Milware: The Implications of State Authored Malicious Software." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2569845.

Herr, Trey, and Bruce Schneier. 2017. "Taking Stock: Estimating Vulnerability Rediscovery." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2928758.

Herzog, Michel, and Jonas Schmid. 2016. "Who Pays for Zero-Days? Balancing Long-Term Stability in Cyber Space against Short-Term National Security Benefits." In *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*, edited by Karsten Friis and Jens Ringsmose, 95–115. London: Routledge.

Hopkins, Michael, and Ali Dehghantanha. 2015. "Exploit Kits: The Production Line of the Cybercrime Economy?" In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*. https://doi.org/10.1109/infosec.2015.7435501.

Hulcoop, Adam, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert. 2017. "Tainted Leaks: Disinformation and Phishing With a Russian Nexus." Citizen Lab. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/.

Internet Engineering Steering Group. 2015. "IESG Statement on Maximizing Encrypted Access To IETF Information." IETF. August 20, 2015. https://www.ietf.org/blog/iesg-statement-maximizing-encrypted-access-ietf-information/?primary_topic=7&.

Johnson, Deborah G., and Kent A. Wayland. 2010. "Surveillance and Transparency as

Sociotechnical Systems of Accountability." In *Surveillance and Democracy*, edited by Kevin D. Haggerty and Minas Samatas, 19–33. New York: Cavendish Publishing.

Keizer, Gregg. 2018. "Browser Updates: Here's How Often Chrome, Firefox, Edge and Safari Get Refreshed." *Computerworld*, June 22, 2018. https://www.computerworld.com/article/3284365/web-browsers/browser-updates-heres-how-often-chrome-firefox-edge-and-safari-get-refreshed.html.

Kerr, Dara. 2017. "FBI Docs Tell How It Hacked San Bernardino Shooter's iPhone, Kind of." *CNet*, January 10, 2017. https://www.cnet.com/news/fbi-docs-tell-how-it-hacked-san-bernardino-shooters-iphone-kind-of/.

Kessler, Mike. 2011. "The Pest Who Shames Companies Into Fixing Security Flaws." *Wired*, November 23, 2011. https://www.wired.com/2011/11/mf_soghoian/.

Koutros, Nicholas, and Julien Demers. 2013a. "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement." *Canadian Journal of Law and Technology* 11 (1): 79.

———. 2013b. "Big Brother's Shadow: Decline in Reported Use of Electronic Surveillance by Canadian Federal Law Enforcement." *Canadian Journal of Law and Technology* 11 (1). https://ojs.library.dal.ca/CJLT/article/view/5998.

Landau, Susan. 2010. *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*. The MIT Press: Cambridge, Mass.

Lewis, James Andrew. 2014. "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage." Center for Strategic International Studies.

Manning, Morris. 1978. *Wiretap Law in Canada: A Supplement to the Protection of Privacy Act, Bill C-176: An Analysis and Commentary*. Toronto: Butterworths.

Marczak, Bill, and John Scott-Railton. 2016. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used against a UAE Human Rights Defender." Citizen Lab, Munk School of Global Affairs and Public Policy at the University of Toronto. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marczak, Bill, John Scott-Railton, and Sarah McKune. 2015. "Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware." Citizen Lab, Munk School of Global Affairs and Public Policy at the University of Toronto. https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/.

Marquis-Boire, Morgan, Bill Marczak, Claudio Guarnieri, and John Scott-Railton. 2013. "You Only Click Twice: FinFisher's Global Proliferation." Citizen Lab, Munk School of Global Affairs at the University of Toronto. https://citizenlab.ca/2013/03/you-only-click-twice-finfishers-global-proliferation-2/.

Maurushat, Alana. 2014. *Disclosure of Security Vulnerabilities: Legal and Ethical Issues*. Springer Science & Business Media.

Molnar, Adam, Christopher Parsons, and Erik Zouave. 2017. "Computer Network Operations and 'Rule-with-Law' in Australia." *Internet Policy Review* 6 (1): 1–14.

Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. 2015. "National CSIRTs and Their Role in Computer Security Incident Response." New America.

Mueller, Milton L. 2010. *Networks and States: The Global Politics of Internet Governance*. MIT Press.

Mulgan, Richard. 1997. ‘‘The Processes of Public Accountability.” Australian Journal of Public Accountability 56(1).

National Defense Act. 1985. *R.S.C.* Vol. c. N-5.

National Security Agency. 2007. “Network Shaping 101.” https://edwardsnowden.com/wp-content/uploads/2016/11/Network-Shaping-101.pdf.

National Security Agency. 2008. “SID Today: 4th Party Collection: Taking Advantage of Non-Partner Computer Network Exploitation Activity.” https://edwardsnowden.com/2015/01/18/4th-party-collection-taking-advantage-of-non-parter-computer-network-exploitation-activity/

National Security Agency. 2010. “DEFIANTWARRIOR and the NSA’s Use of Bots.” https://edwardsnowden.com/wp-content/uploads/2015/01/media-35689.pdf.

National Security Agency. 2016. “Network Shaping 101.” https://edwardsnowden.com/docs/doc/Network-Shaping-101.pdf.

Newman, Lily Hay. 2016. “A Top-Shelf iPhone Hack Now Goes For $1.5 Million.” *Wired*, September 26, 2016. https://www.wired.com/2016/09/top-shelf-iphone-hack-now-goes-1-5-million/.

Osborne, Charlie. 2017. “Zerodium lures researchers with $1 million payout for Tor Browser flaws.” *ZDNet*, September 14, 2017. https://www.zdnet.com/article/zerodium-lures-researchers-with-1-million-payout-for-tor-browser-flaws/.

Parsons, Christopher. 2015. ‘‘Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance.” *Media and Communication* 3(3).

Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert. 2017a. “Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).” Citizen Lab, Munk School of Global Affairs and Public Policy at the University of Toronto. https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf.

———. 2017b. “Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).” Citizen Lab, Munk School of Global Affairs and Public Policy at the University of Toronto. https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf.

Parsons, Christopher, and Adam Molnar. 2018. “Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports.” *Canadian Journal of Law and Technology* 16 (1): 143–69.

Pelizzo, Riccardo, and Frederick Stapenhurst. 2013. *Government Accountability and Legislative Oversight*. Routledge.

Pell, Stephanie K., and James Finocchiaro. 2017. “The Ethical Imperative for Common Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid That Process.” *Connecticut Law Review* 49: 1549.

Perrow, Charles. 2011. *Normal Accidents: Living with High Risk Technologies*. Princeton University Press.

Peter Margulies, and Peter Margulies. 2017. “Global Cybersecurity, Surveillance, and Privacy: The Obama Administration’s Conflicted Legacy.” *Indiana Journal of Global Legal Studies*

24 (2): 459.
Porteous, Holly. 2018. “Cybersecurity: Technical and Policy Challenges.” Publication No. 2018-05-E. Library of Parliament.
Rid, Thomas, and Ben Buchanan. 2014. “Attributing Cyber Attacks.” *Journal of Strategic Studies* 38 (1-2): 4–37.
Roach, Kent. 2015. ‘‘Permanent Accountability Gaps and Partial Remedies.” In Michael Geist, ed., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press.
Savage, Charlie. 2015. *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*. Little, Brown.
Schedler, Andreas. 1999. ‘‘Conceptualizing Accountability.” In Andreas Schedler, Larry Diamond & Marc Plattner, eds., *The Self-Restraining State: Power and Accountability in New Democracies*. Boulder: Lynne Rienner.
Schneier, Bruce. 2016. “Cryptography Is Harder Than It Looks.” *IEEE: Security and Privacy,* January/February.
Segal, Adam. 2013. “The Code Not Taken: China, the United States, and the Future of Cyber Espionage.” *The Bulletin of the Atomic Scientists* 69 (5): 38–45.
Shane, Scott, Nicole Perlroth, and David E. Sanger. 2017. “Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core.” *New York Times*, November 12, 2017. https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.
Shepardson, David. 2016. “U.S. investigates security of mobile devices.” *Reuters*, May 9, 2016. https://www.reuters.com/article/us-wireless-inquiry-regulators-idUSKCN0Y022E.
Shezaf, Hagar, and Jonathan Jacobson. 2018. “Revealed: Israel’s Cyber-Spy Industry Helps World Dictators Hunt Dissidents and Gays.” *Haaretz*, October 20, 2018. https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027.
Snow, John. 2016. “Petya Ransomware Eats Your Hard Drives.” *Kaspersky Lab Daily*, March 30, 2016. https://www.kaspersky.com/blog/petya-ransomware/11715/.
Spanos, Georgios, Lefteris Angelis, and Kyriaki Kosmidou. 2017. “Is the Market Value of Software Vendors Affected by Software Vulnerability Announcements?” In *Springer Proceedings in Business and Economics*, 465–69.
SpiderLabs Research. 2016. “Zero Day Auction for the Masses.” *Trustwave*, June 9, 2016. https://www.trustwave.com/Resources/SpiderLabs-Blog/Zero-Day-Auction-for-the-Masses/.
Spiegel Staff. 2013. “Unit Offers Spy Gadgets for Every Need.” *Der Spiegel*, December 30, 2013. http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html.
Brenner, Susan W.; Crescenzi, Anthony C. 2006. “State-Sponsored Crime: The Futility of the Economic Espionage Act.” *Houston Journal of International Law* 28 (2): 389–466.
Stevens, Tim. 2017. “Cyberweapons: Power and the Governance of the Invisible.” *International Politics* 55 (3-4): 482–502.
Strobel, Warren. 2018. “Pentagon’s Cyber Command Gets Upgraded Status, New Leader.” *Reuters*, May 4, 2018. https://www.reuters.com/article/us-usa-defense-cyber/pentagons-

cyber-command-gets-upgraded-status-new-leader-idUSKBN1I52MS.
United States Government. 2018. “National Cyber Strategy of the United States of America.” United states of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
Verizon. 2016. “ 2016 Data Breach Investigations Report.” Verizon Enterprise. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.
Wikileaks. 2017. “Vault 7: CIA Hacking Tools Revealed.” Wikileaks. March 7, 2017. https://wikileaks.org/ciav7p1/.
Watson, Kathryn. 2018. “Russian Intelligence Officers Indicted in DNC Hacking.” *CBS News*, July 13, 2018. https://www.cbsnews.com/news/deputy-attorney-general-rod-rosenstein-makes-announcement-live-updates/.
Wilson, Andi, Ross Schulman, Kevin Bankston, and Trey Herr. 2016. “Bugs in the System: A Primer on the Software Vulnerability Ecosystem and Its Policy Implications.” New America.
Wilson, Clay. 2014. “Cyber Threats to Critical Information Infrastructure.” In *Cyberterrorism*, 123–36.
Winner, Langdon. 1988. *The Whale and the Reactor*.
Wolf, Marty J., and Nir Fresco. 2016. “Ethics of the Software Vulnerabilities and Exploits Market.” *The Information Society* 32 (4): 269–79.
Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. Crown.
Zhao, Mingyi, Jens Gorssklags, and Peng Liu. 2015. “An Empirical Study of Web Vulnerability Discovery Ecosystems.” In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 1105–17.