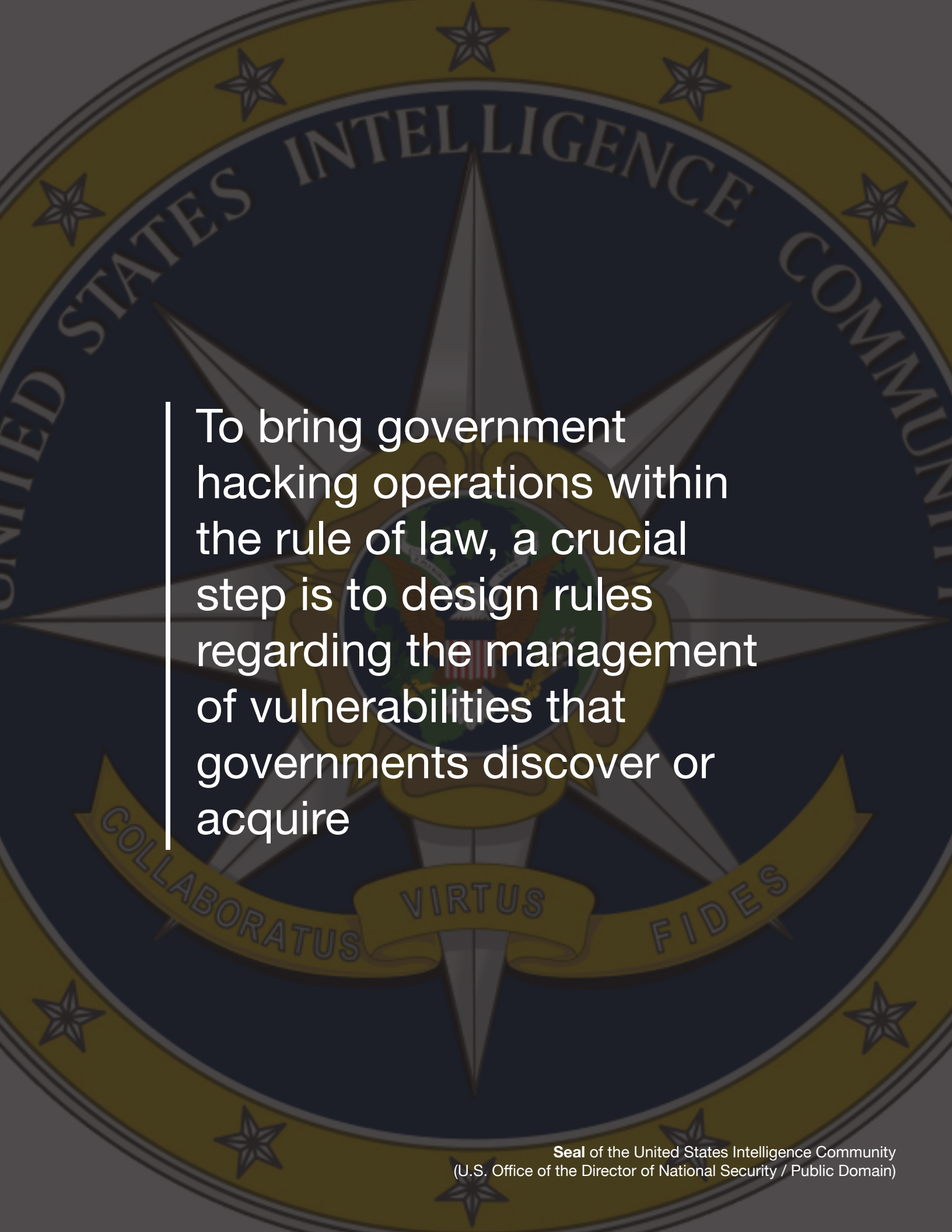

To bring government hacking operations within the rule of law, a crucial step is to design rules regarding the management of vulnerabilities that governments discover or acquire

Seal of the United States Intelligence Community
(U.S. Office of the Director of National Security / Public Domain)

The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes

Sharon Bradford Franklin

In 2017, leaders of the U.S. Intelligence Community warned that "more than 30 nations are developing offensive cyberattack capabilities."[1] This means that more than 30 countries may be conducting hacking operations as a method for surveillance, disruption, or destruction. Unregulated cyber surveillance and cyberattacks by government actors can pose risks not only to a government's foreign adversaries, but also to its own citizens. Thus, as the United States and other nations work to enhance their own offensive cyber capabilities, as well as to develop strategies to defend against potential attacks, it is critical that these countries establish legal regimes to govern such conduct in cyberspace. Although Germany has established a legal framework to regulate government hacking activities,[2] few countries have done so.[3]

To bring government hacking operations within the rule of law, a crucial step is to design rules regarding the management of vulnerabilities that governments discover or acquire. As with other cyber actors, when governments conduct hacking operations, this frequently involves exploiting vulnerabilities in computer hardware and software systems. But these same flaws can also be manipulated by a government's foreign adversaries or other malicious actors. Therefore, when countries consider their abilities to rely on hacking as an investigative tool, as well as their interests in exploiting vulnerabilities for military and intelligence operations, they must also evaluate the capacity of information and communications technology providers to repair bugs and protect the cybersecurity of all users. Determining whether to exploit a vulnerability or disclose it to a vendor for patching involves balancing a variety of different security concerns against each other.

Some countries have made progress in formalizing the rules for making these decisions and in publicizing these rules to promote public accountability. In November 2017, the United States released a charter governing its Vulnerabilities Equities Process (VEP), which outlines how the U.S. government weighs the various competing equities.[4] The charter delineates which components of the government will participate in determinations regarding whether to disclose or retain each newly discovered vulnerability, and it sets forth the criteria to be used and the process to be followed in making such assessments. One year later, the United Kingdom (UK) announced its Equities Process, which follows a similar approach.[5] Most recently, in March 2019, Australia released its "Responsible Release Principles for Cyber Security Vulnerabilities,"[6] and Germany is currently working to develop a VEP and is expected to make information about its process public in early 2019.[7] However, as described below, the VEP procedures revealed to date need further improvement,[8] and most of the nations with offensive cyber capabilities have not developed—or at least have not announced—any such framework.

There are several reasons why countries should develop, formalize, and publicize VEP procedures. First, as noted above, creating a VEP is a critical step toward bringing government hacking within the rule of law. Much more work is needed, particularly in the United States, to clarify and limit the authority of government actors to engage in hacking.[9] Nonetheless, clear rules for vulnerability management, transparency regarding the decision-making process, and public reporting of statistics regarding the frequency with which vulnerabilities are disclosed and retained can help hold governments accountable to their citizens. Second, as more countries develop VEP procedures, this can assist nations in cooperating to combat the threats posed by various malicious cyber actors and can help establish international norms. Widespread adoption and publication of VEP rules can facilitate information sharing among countries about common cyber threats, as the United Kingdom has recognized in its Equities Process document, noting that vulnerabilities may not be subject to formal review if they "have already been subjected to similar considerations by a partner and shared with us."[10] Third, governments will benefit from formalizing decision making to evaluate the security versus security tradeoffs involved

in handling vulnerabilities. These are not easy decisions, and, as the "E" in "VEP" recognizes, there are many different "equities" to be assessed in determining when a vulnerability should be disclosed to the vendor for patching. In particular, a VEP can ensure that the interest in disclosing vulnerabilities for repair to promote the cybersecurity of all users will receive appropriate weight and that it will not be lost in the pressured and secretive environment of classified conversations among a limited number of intelligence or military officials.

This last point is worth emphasizing as a critical role to be played by VEP procedures. Despite widespread recognition of the cybersecurity risks posed when governments stockpile vulnerabilities,[11] there can be a natural inclination by law enforcement, intelligence, and military officials to press for retention and exploitation. To ensure a robust VEP that truly weighs all relevant equities, the decision-making process must include adequate representation from government agencies or actors that will press for disclosure and repair of vulnerabilities to promote the public's cybersecurity. For example, the U.S. VEP review board includes the Department of Commerce and the National Cybersecurity Communications and Integration Center, both of which can provide a perspective focused on protecting digital security for all users. Because different nations vary in the structure of their cyber-related operations, VEP procedures should be tailored to individual countries to provide for such representation. The procedures should also ensure that the voices counseling in favor of disclosure and repair will not be regularly drowned out by those urging retention and exploitation.

Although the structure of VEP review boards will likely vary from country to country, there are some critical elements that should be included in any VEP, and the U.S. VEP, the UK Equities Process, and the Australian Responsible Release Principles share certain important features. All three documents explicitly start from the premise that, in most cases, disclosing a vulnerability for repair is in the country's national interest. Promptly disclosing a newly discovered vulnerability to the manufacturer allows companies to develop patches and protect the cybersecurity of all users. As the Australian Responsible Release Principles state: "Our starting position is simple: when we find a weakness, we disclose it."[12] Similarly, all three processes require that any government decision to retain and exploit a vulnerability must be periodically reevaluated on at least an annual basis. Governments must recognize that the vulnerabilities they retain can also be discovered and exploited by their adversaries, and, over time, the cybersecurity risks of leaving vulnerabilities unpatched will continue to grow. As stated in a recent policy paper by the German think tank Stiftung Neue Verantwortung (SNV), VEP policies should determine "'when' and 'how' disclosure should occur rather than 'whether' and 'if.'"[13]

There are also some challenges that are common to any VEP. One difficult issue is the question of whether it should be permissible to exclude a vulnerability from the evaluation process based on a nondisclosure agreement (NDA) with a private vendor. Many countries obtain vulnerabilities by purchasing them from private companies rather than through their own research, and these vendors typically demand NDAs so they can continue to sell the vulnerabilities to other purchasers. Although there is little public information about the scope of this gray market,[14] the U.S. VEP explicitly states that determinations under the process "could be subject to restrictions by partner agreements and sensitive operations."[15] This exclusion of vulnerabilities acquired under NDAs from VEP review threatens to become an exception that swallows the rule. The U.S. government should remove this exemption and require

United States President Barack Obama tours the National Cybersecurity and Communications Integration Center (Pete Souza / Public Domain)

vulnerabilities to be assessed through the VEP, regardless of whether they were discovered by government agencies or purchased from vendors. As some former government officials involved in this process have argued, the government could limit its purchases from vendors to cases where it buys the exclusive rights to a vulnerability, and it could regularly reevaluate these vulnerabilities through the VEP.[16]

Finally, there is the challenge of providing transparency. Certain information about the application of a VEP will appropriately remain classified, such as the nature of vulnerabilities currently being retained for exploitation. But transparency—at least for the applicable rules of the VEP and for statistical information regarding the number of vulnerabilities considered, disclosed and retained—is critical to the legitimacy and successful operation of any VEP. The U.S. VEP charter requires annual reporting, including "statistical data as deemed appropriate,"[17] but the charter does not commit the government to providing its annual report to Congress or the public. Similarly, the Australian Responsible Release Principles state that the Australian Signals Directorate submits annual reports to the Inspector-General and the Minister for Defence, but they do not contain any provision regarding public reporting.[18] The UK Equities Process is completely silent on the issue of transparency reporting. A requirement for regular public reporting should be a high-priority area for improvement to these existing VEP procedures.

The United States, the United Kingdom, and Australia should continue to develop and refine their vulnerabilities review procedures to ensure that all newly discovered vulnerabilities are considered through a robust process that is accountable to the public. Meanwhile, the models provided by these countries are good places for other countries to start. As nations strive to improve their cyber capabilities and grapple with how to best protect their populations and their resources, they should also ensure that their actions are conducted in accordance with the rule of law. Creating clear rules and providing transparency about the management of vulnerabilities can be an important first step in this critical effort.

---

[1] James R. Clapper, Marcel Lettre, and Michael S. Rogers, *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*, 115th Cong., 1st sess., January 5, 2017.
[2] The German Code of Criminal Procedure § 100 (2014).
[3] Alex Betschen, "We're Suing the Government to Learn Its Rules for When It Hacks Into People's Devices," American Civil Liberties Union, December 21, 2018, <https://www.aclu.org/blog/privacy-technology/internet-privacy/were-suing-government-learn-its-rules-when-it-hacks-peoples>.
[4] *Vulnerabilities Equities Policy and Process for the United States Government*, White House document, November 15, 2017.
[5] "The Equities Process," GCHQ, November 29, 2018, <https://www.gchq.gov.uk/features/equities-process>.
[6] "Responsible Release Principles for Cyber Security Vulnerabilities," Australian Signals Directorate, March 2019, <https://asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf>.
[7] Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World," *Lawfare*, January 4, 2019, <https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world>.
[8] Sharon Bradford Franklin and Andi Wilson, "Rules of the Road: The Need for Vulnerabilities Equities Legislation," *Lawfare,* November 22, 2017, <https://www.lawfareblog.com/rules-road-need-vulnerabilities-equities-legislation>.
[9] Kevin Bankston, "Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors," *Lawfare,* June 14, 2017, <https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors>.
[10] "The Equities Process."
[11] Ellen Nakashima and Andrea Peterson, "NSA's use of software flaws to hack foreign targets posed risks to cybersecurity," *The Washington Post,* August 17, 2016, <https://www.washingtonpost.com/world/national-security/nsas-use-of-software-flaws-to-hack-foreign-targets-posed-risks-to-cybersecurity/2016/08/17/657d837a-6487-11e6-96c0-37533479f3f5_story.html>; and "Governments need to do more, and say more, on vulnerability handling," The Cybersecurity Tech Accord, September 10, 2018, <https://cybertechaccord.org/government-vulnerability-handling>.
[12] "Responsible Release Principles for Cyber Security Vulnerabilities."
[13] Sven Herpig, *Governmental Vulnerability Assessment and Management* (Berlin: Stiftung Neue Verantwortung, August 2018), 3.
[14] Rhys Dipshan, "The Federal Policy Loophole Supporting the Hacking-for-Hire Market," *Future Tense*, June 20, 2018, <https://slate.com/technology/2018/06/the-federal-policy-loophole-supporting-the-hacking-for-hire-market.html>.
[15] *Vulnerabilities Equities Policy and Process for the United States Government*, 9.
[16] Ari Schwartz and Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process* (Cambridge: The Cyber Security Project at the Belfer Center for Science and International Affairs, June 15, 2016), 15.
[17] *Vulnerabilities Equities Policy and Process for the United States Government*, 5.
[18] "Responsible Release Principles for Cyber Security Vulnerabilities," 1.

Sharon Bradford Franklin

Sharon Bradford Franklin is Director of Surveillance & Cybersecurity Policy at New America's Open Technology Institute (OTI). She leads OTI's work on issues involving government surveillance, encryption, cybersecurity, government access to data, transparency, and freedom of expression online. From 2013 to 2017, she served as Executive Director of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent federal agency that reviews counterterrorism programs to ensure that they include appropriate safeguards for privacy and civil liberties. Previously, she served as Senior Counsel at the Constitution Project, a nonprofit legal watchdog group, working on a range of issues involving national security and privacy and civil liberties. Franklin is a graduate of Harvard College and Yale Law School.