4-2017

Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web

Ahmed Ghappour
Boston University School of Law

Stanford Law Review

Volume 69 April 2017

ARTICLE

Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web

Ahmed Ghappour*

Abstract. The use of hacking tools by law enforcement to pursue criminal suspects who have anonymized their communications on the dark web presents a looming flashpoint between criminal procedure and international law. Criminal actors who use the dark web (for instance, to commit crimes or to evade authorities) obscure digital footprints left behind with third parties, rendering existing surveillance methods obsolete. In response, law enforcement has implemented hacking techniques that deploy surveillance software over the Internet to directly access and control criminals' devices. The practical reality of the underlying technologies makes it inevitable that foreign-located computers will be subject to remote "searches" and "seizures." The result may well be the greatest extraterritorial expansion of enforcement jurisdiction in U.S. law enforcement history.

This Article examines how the government's use of hacking tools on the dark web profoundly disrupts the legal architecture on which cross-border criminal investigations rest. These overseas cyberoperations raise increasingly difficult questions regarding who may authorize these activities, where they may be deployed, and against whom they may lawfully be executed. The rules of criminal procedure fail to regulate law enforcement hacking because they allow these critical decisions to be made by rank-and-file officials despite potentially disruptive foreign relations implications. This Article outlines a regulatory framework that reallocates decisionmaking to the institutional actors who are best suited to determine U.S. foreign policy and avoids sacrificing law enforcement's ability to identify and locate criminal suspects who have taken cover on the dark web.

* Visiting Assistant Professor, U.C. Hastings College of the Law. For helpful conversations, comments, and support, I thank Ryan Calo, Anupam Chander, Bobby Chesney, Danielle Citron, Jennifer Daskal, Bill Dodge, Scott Dodson, Derek Jinks, Elizabeth Joh, Orin Kerr, Rick Marcus, Tara Mikkilineni, Paul Ohm, Austen Parrish, Stephanie K. Pell, Morris Ratner, Bertrall Ross, Reuel Schiller, Chris Soghoian, David Sloss, and Katherine Strandburg. I also thank participants in workshops and conferences at American University Washington College of Law, U.C. Berkeley School of Law, U.C. Davis School of Law, U.C. Hastings College of the Law, N.Y.U. School of Law, the U.S. Military Academy, and Yale Law School for their helpful comments and conversations. Finally, I thank the editors of the *Stanford Law Review* for their terrific editing.

Searching Places Unknown
69 STAN. L. REV. 1075 (2017)

Table of Contents

Introduction

Nestled deep beneath the surface of the World Wide Web, Dread Pirate Roberts (DPR) ran an underground empire of criminality. Not much was known about DPR, except that he appeared to have built the Silk Road—a global online marketplace for illicit services and contraband.[1] DPR—later identified as Ross Ulbricht—was the target of a global manhunt that operated in the dark for nearly three years.[2] In that time, the Silk Road attracted over 100,000 users who transacted over one million deals, generating an estimated $1.2 billion in global sales from vendors located in more than ten countries around the world.[3]

The Silk Road was built to facilitate black market transactions. It was hosted on the dark web, a global network of computers that use a cryptographic protocol to communicate, enabling users to conduct transactions anonymously without revealing their location.[4] Users could only make payments in the digital currency Bitcoin, and transactions were run through a "series of dummy transaction[s] to disguise the link between buyers and

1. MARC GOODMAN, FUTURE CRIMES: EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE, AND WHAT WE CAN DO ABOUT IT 194 (2015); Press Release, U.S. Att'y's Office for the S. Dist. of N.Y., U.S. Dep't of Justice, Ross Ulbricht, A/K/A "Dread Pirate Roberts," Sentenced in Manhattan Federal Court to Life in Prison (May 29, 2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

2. The Silk Road website went live in February 2011. *See* GOODMAN, *supra* note 1, at 198. U.S. agencies commenced a number of independent Silk Road investigations in the fall of 2011. *See, e.g.*, Transcript of Trial at 1389, United States v. Ulbricht, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 28, 2015) (relating a joint stipulation by the government and defense that if called to testify, Special Agent Richardson of the Drug Enforcement Administration would testify that she attempted a number of purchases on the Silk Road website between September 2011 and May 2013 as part of an undercover investigation); Transcript of Trial at 71, 153, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 14, 2015) (indicating via in-court testimony that the U.S. Department of Homeland Security (DHS) commenced its investigation in October 2011); Affidavit of Special Agent Ilhwan Yum in Support of a Search Warrant at 1, 6, United States v. Certain Premises, No. 13-1051-M (E.D. Pa. Sept. 9, 2013) (stating that an investigation by the Federal Bureau of Investigation (FBI) was ongoing as of November 2011). Ulbricht was arrested on October 1, 2013. *See* Affidavit of Special Agent Tigran Gambaryan in Support of Criminal Complaint at 11, United States v. Force, No. 3-15-70370 (N.D. Cal. Mar. 25, 2015). The Silk Road was shuttered by the FBI on October 2, 2013. *See id.* at 10.

3. *See* Press Release, U.S. Att'y's Office for the S. Dist. of N.Y., *supra* note 1; *see also* Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014, 2:54 PM EDT), http://usat.ly/1b8Gntk ("Beyond illegal drugs, the site served as a bazaar for fake passports, driver's licenses and other documents, as well as illegal service providers, such as hit men, forgers and computer hackers.").

4. Leger, *supra* note 3. To access the Silk Road, users needed specialized anonymity software allowing them to communicate on the dark web. *Id.*

sellers."[5] Thousands of drug dealers flocked to the Silk Road because of the anonymity it promised;[6] there, they conducted over a million drug deals out of reach of law enforcement's most advanced electronic surveillance tools.[7]

Investigators made bold efforts to infiltrate the hidden website to identify DPR. They posed as buyers and sellers on the site, completing over a hundred purchases.[8] One agent even infiltrated the staff of the website, spending ten to twelve hours per day administering the site and communicating with DPR directly.[9] All for naught. Their attempts failed because existing surveillance methods rely on digital trails left behind with third parties by computers on the web—the very information obscured by the dark web. In the end, it was an IRS agent who solved the case, stumbling upon communications on a public website advertising the Silk Road just before its launch in 2011.[10] Because of Ulbricht's own human error, the communication was traced back to him,[11] and the alleged kingpin was apprehended, prosecuted, and sentenced to life in prison.[12]

Several underground marketplaces surfaced in the wake of the Silk Road,[13] highlighting an asymmetry between investigators' ability to track unlawful activity and criminals' capacity to commit crimes on the dark web.[14] The

5. *Id.*

6. *See* Transcript of Trial at 42, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. Jan. 13, 2015) ("Thousands of drug dealers flocked to Silk Road, and more than 1 million drug deals took place on the site before the government shut it down.").

7. *See id.*; Leslie R. Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation*, U.S. DEP'T JUST. BLOGS (Nov. 21, 2016), https://www.justice.gov/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation ("[T]he abuse of internet anonymizing technology . . . [is] the digital equivalent of crimes committed in the middle of a busy street, in full view of the citizenry and the police, with little risk of being caught." (italics omitted)).

8. *See* GOODMAN, *supra* note 1, at 196.

9. *See* Andy Greenberg, *Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht*, WIRED (Jan. 14, 2015, 6:34 PM), https://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht.

10. *See* Nathaniel Popper, *The Tax Sleuth Who Took Down a Drug Lord*, N.Y. TIMES: DEALBOOK (Dec. 25, 2015), http://nyti.ms/1R02DMZ.

11. *See id.*

12. *See* Transcript of Sentencing at 94, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. May 29, 2015). In the interest of disclosure, the Author advised on Ulbricht's appeal.

13. *See, e.g.*, Steven Nelson, *Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road*, U.S. NEWS & WORLD REP. (Oct. 2, 2015, 3:12 PM), http://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road; Benjamin Weiser, *Man Charged with Operating Silk Road 2.0, a Black Market Website*, N.Y. TIMES (Nov. 6, 2014), http://nyti.ms/1slvgVH.

14. For example, Senator Tom Carper (D-Del.), then-Chairman of the Senate Homeland Security and Governmental Affairs Committee, stated at the time of the launch of Silk Road 2.0: "This new website—launched barely a month after Federal agents shut down

footnote continued on next page

existence of hidden services like the Silk Road "dramatically lower[s] the entry barriers into the underground economy—for both buyers and sellers" of illicit goods and services.[15] The use of the dark web by criminal actors therefore enables secret, untraceable criminal activity to take place at scale. This has led policymakers to question whether law enforcement has sufficient tools to counter the illicit conduct that might flow through the digital underworld.[16]

The term "network investigative technique" is a euphemism for law enforcement hacking; it describes a law enforcement surveillance method that entails remotely accessing and installing malware on a computer without the permission of its owner or operator.[17] Network investigative techniques are especially useful in the pursuit of criminal suspects who use anonymizing software to obscure their location. By accessing the target computer directly and converting it into a surveillance device, use of network investigative techniques circumvents the need to know a target's location and makes the

---

the original Silk Road—underscores the inescapable reality that technology is dynamic and ever-evolving and that government policy needs to adapt accordingly." Press Release, Sen. Tom Carper, Chairman, Senate Homeland Sec. & Governmental Affairs Comm., Chairman Carper Statement on the Unveiling of the So-Called "Silk Road 2.0" Website (Nov. 6 2013), https://www.hsgac.senate.gov/media/majority-media/chairman-carper-statement-on-the-unveiling-of-the-so-called-silk-road-20-website.

15. *See* Government Sentencing Submission at 2, *Ulbricht*, No. 14 Cr. 68 (KBF) (S.D.N.Y. May 26, 2015).

16. *See, e.g.*, Press Release, Sen. Tom Carper, *supra* note 14.

17. This Article uses the terms "network investigative technique," "cyberexfiltration operation," and "hacking" interchangeably to describe the use of software that subverts a computer. In computer science, the common term is "malware" (short for "malicious software"). *See* ROBERT SLADE, DICTIONARY OF INFORMATION SECURITY 118 (2006) (defining malware as a "collective term including the many varieties of deliberately malicious software; that is, software written for the purpose of causing inconvenience, destruction, or the breaking of security policies or provisions"). Law enforcement has used a wide variety of other terms to refer to hacking, including "Computer and Internet Protocol Address Verifier" (CIPAV), "Internet Protocol Address Verifier" (IPAV), "Remote Access Search and Surveillance" (RASS), "Remote Computer Search," "Remote Search," "Computer Tracer," "Internet Tracer," "Remote Computer Trace," and "Web Bug." *See, e.g.*, Application & Affidavit of Special Agent Norman B. Sanders, Jr. for Search Warrant at 2-3, *In re* Search of Any Comput. Accessing Elec. Messages Directed to MySpace Account "Timberlinebombinfo," No. MJ07-5114 (W.D. Wash. June 12, 2007) [hereinafter Sanders Affidavit] (using "CIPAV"); *see also* Elec. Frontier Found., FBI CIPAV-8 (n.d.), https://www.eff.org/files/filenode/cipav/fbi_cipav-08.pdf (consisting of a cache of documents released from the FBI to the Electronic Frontier Foundation showing usage of the terms "CIPAV," "IPAV," "RASS," and "Web Bug" in various FBI correspondences and field office requests for technical assistance from the FBI's Cryptologic and Electronic Analysis Unit); Elec. Frontier Found., FBI CIPAV-10 (n.d.), https://www.eff.org/files/filenode/cipav/FBI_CIPAV-10.pdf (consisting of a cache of documents released from the FBI to the Electronic Frontier Foundation showing usage of these terms in various FBI field office requests for technical assistance from the FBI's Cryptologic and Electronic Analysis Unit).

new surveillance method a practical solution for the pursuit of criminal suspects on the dark web. Once installed, the right malware can cause a computer to perform any task the computer is capable of performing.[18] Malware can force the target computer to covertly upload files to a server controlled by law enforcement or instruct the computer's camera or microphone to gather images and sound.[19] It can even commandeer computers that associate with the target by, for example, accessing a website it hosts.[20]

The legal process for the use of network investigative techniques is governed by Federal Rule of Criminal Procedure 41, which articulates procedures for obtaining a search warrant in federal magistrate court. The former version of Rule 41 restricted authority to issue search warrants to the district of the magistrate making the decision.[21] This had caused courts to deny search warrants for computers whose locations were unknown because they may have been outside the magistrate's district.[22] An amendment to the rule laid to rest this administrative hurdle by explicitly permitting magistrates to issue a search warrant for a device if the device's location "has been concealed through technological means."[23] The relevant portion of Rule 41(b)(6) reads:

18. *See What Is Malware?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/documentation/glossary/what-is-malware (last visited Apr. 4, 2017) (defining "malware" as "a file or code, typically delivered over a network[,] that infects, explores, steals or conducts virtually any behavior an attacker wants"); *see also* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 26-27 (2014) (providing a brief technical explanation of how malware can control devices and components of a computer by modifying programs known as "device drivers"); Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST (Dec. 6, 2013), https://wpo.st/dooc2 (describing the functionality of various types of malware known to have been used by the FBI).

19. *See In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013) (rejecting an application for a warrant to deploy malware "designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period"); Timberg & Nakashima, *supra* note 18 (describing malware that turns on a computer's camera); Kim Zetter, *So . . . Now the Government Wants to Hack Cybercrime* Victims, WIRED (May 4, 2016, 7:00 AM), https://www.wired.com/2016/05/now-government-wants-hack-cybercrime-victims (describing malware that turns on a computer's microphone).

20. *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), http://www.wired.com/2014/08/operation_torpedo.

21. *See* FED. R. CRIM. P. 41(b)(1)-(5). Rule 41 provides that a search warrant may be issued by "a magistrate judge with authority in the district." *See id.* 41(b).

22. *See, e.g.*, *In re Warrant to Search a Target Comput. at Premises Unknown*, 958 F. Supp. 2d at 757, 761.

23. *See* Letters from Chief Justice John G. Roberts to Paul D. Ryan, Speaker, U.S. House of Representatives, and Joseph R. Biden, Jr., President, U.S. Senate, attachment at 6 (Apr. 28, 2016), https://www.supremecourt.gov/orders/courtorders/frcr16_mj80.pdf (submitting amendments to the Federal Rules of Criminal Procedure).

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located *within or outside* that district if:
>
> (A) the district where the media or information is located has been concealed through technological means . . . .[24]

Although the U.S. Department of Justice (DOJ), in recommending the amendment to Rule 41, explicitly stated that the amendment is not meant to give courts the power to issue warrants that authorize searches in foreign countries,[25] the practical reality of the underlying technology means overseas searches will be both unavoidable and frequent. The result may well be the largest expansion of extraterritorial enforcement jurisdiction in FBI history.[26]

The legal process for network investigative techniques presumes search targets are territorially located, which is not at all accurate. Indeed, most potential targets on the dark web are *outside* the territorial United States.[27] Approximately 80% of the computers on the dark web are located outside the United States.[28] And because each device's location is indistinguishable from that of the next, any given law enforcement target is likely to be located

24. FED. R. CRIM. P. 41(b)(6) (emphasis added). The amendment became effective on December 1, 2016. *See id.* advisory committee's note to 2016 amendment.

25. *See* Letter from Mythili Raman, Acting Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice, to Judge Reena Raggi, Chair, Advisory Comm. on Rules of Criminal Procedure 4 (Sept. 18, 2013), *in* ADVISORY COMM. ON CRIMINAL RULES, ADVISORY COMMITTEE ON RULES OF CRIMINAL PROCEDURE: APRIL 2014, at 171, 174 (2014), http://www.uscourts.gov/sites/default/files/fr_import/CR2014-04.pdf.

26. *See* Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (Sept. 16, 2014, 9:10 AM), http://justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance.

27. For example, in the Silk Road case, computer security experts who were following or associated with the case opined that it was possible the FBI hacked into Silk Road servers, located in Iceland, to extract key evidence used in the prosecution and forfeiture proceedings. *See, e.g.*, Joseph Cox, *How Did the FBI Find the Silk Road Servers, Anyway?*, MOTHERBOARD (Oct. 3, 2014, 8:55 AM), http://motherboard.vice.com/read/how-did-the-fbi-find-the-silk-road-servers-anyway. This issue was raised by the defense and denied on standing grounds and is currently on appeal. *See* Brief for Defendant-Appellant at 108, United States v. Ulbricht, No. 15-1815-CR (2d Cir. Jan. 12, 2016), 2016 WL 158389; *see also* Andy Greenberg, *Fed's Silk Road Investigation Broke Privacy Laws, Defendant Tells Court*, WIRED (Aug. 2, 2014, 2:54 PM), https://www.wired.com/2014/08/feds-silk-road-investigation-violated-privacy-law-sites-alleged-creator-tells-court. More recently, as part of a child pornography investigation the FBI infected thousands of computers overseas with malware. *See* Joseph Cox, *FBI Hacked Over 8,000 Computers in 120 Countries Based on One Warrant*, MOTHERBOARD (Nov. 22, 2016, 6:18 PM EST) [hereinafter Cox, *FBI Hack*], http://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

28. *See Top-10 Countries by Relay Users*, TORMETRICS, https://metrics.torproject.org/userstats-relay-table.html (last visited Apr. 4, 2017).

abroad. Thus, the issue is not whether magistrates should be authorized to issue search warrants where the target of the search can be in any of the ninety-four federal judicial districts in the United States. Instead, the issue is whether (and how) investigators should conduct out-of-district searches where targets are likely to be located *out-of-country* as well.

The extraterritorial aspect of law enforcement hacking operations has drawn sharp public criticism by a wide array of commentators, academics, civil liberties organizations, and technology corporations.[29] Technology giant Google warned that the use of network investigative techniques in pursuit of targets on the dark web would undermine the sovereignty of nations by "authorizing the government to conduct searches outside the United States."[30] Google and others cautioned that loosening territorial restrictions on the government's search and seizure power "raises a number of monumental and highly complex constitutional, legal, and geopolitical concerns."[31] While the Advisory Committee on Rules of Criminal Procedure flagged this concern,[32] noting the potential regulatory gap regarding cross-border searches, it explicitly left such "issues that may have foreign policy implications" to be dealt with through "inter-executive branch coordination."[33]

Whether law enforcement is permitted to launch cross-border cyberexfiltration operations is the latest in a series of questions testing the limits of unilateral investigatory activities in a globally networked world. At the core of the inquiry is the well-established international law axiom that one state may

29. The Rule 41 Subcommittee received more than fifty written comments in addition to comments that were presented at hearings before the full Advisory Committee in November 2014. *See Proposed Amendments to the Federal Rules of Criminal Procedure*, REGULATIONS.GOV, https://www.regulations.gov/docketBrowser?rpp=25&so=DESC&sb=commentDueDate&po=0&D=USC-RULES-CR-2014-0004 (last visited Apr. 4, 2017). Civil liberties groups that submitted public comments included the ACLU, the Center for Democracy & Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the National Association of Criminal Defense Lawyers. *See id.*

30. Letter from Richard Salgado, Dir. of Law Enf't & Info. Sec., Google Inc., to the Advisory Comm. on Rules of Criminal Procedure 2-3 (Feb. 13, 2015), https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0029&attachmentNumber=1&contentType=pdf.

31. *Id.* at 1; *see also, e.g.*, Ctr. for Democracy & Tech., Written Statement of the Center for Democracy & Technology Before the Advisory Committee on Rules of Criminal Procedure 4 (2014), http://www.regulations.gov/#!documentDetail;D=USC-RULES-CR-2014-0004-0009 ("Unilateral extraterritorial searches may violate the international obligations of the United States.").

32. *See* Memorandum from Sara Sun Beale & Nancy King, Reporters, to Advisory Comm. on Rules of Criminal Procedure 13-14 (Feb. 25, 2015), *in* ADVISORY COMM. ON CRIMINAL RULES, ADVISORY COMMITTEE ON RULES OF CRIMINAL PROCEDURE: MAY 2015, at 87, 99-100 (2015), http://www.uscourts.gov/sites/default/files/fr_import/CR2015-05.pdf.

33. *Id.* at 14-15.

not unilaterally exercise its law enforcement functions in the territory of another state,[34] which has not been adequately addressed by courts or scholarship in the context of cyberspace.

While there is a wealth of scholarship on the relationship between the Internet and state sovereignty, its focus has almost exclusively been on the permissibility of one state's laws regulating Internet conduct that takes place in another state (exercising "prescriptive jurisdiction"), rather than the permissibility of a state effectuating compliance with those laws in the territory of another state (exercising "enforcement jurisdiction").[35] Jack Goldsmith offers perhaps the most sustained focus on the issue of cross-border enforcement jurisdiction. He argues that while multiple nations may in theory regulate the same Internet transaction, the system as a whole is stable in part because each nation can only *enforce* regulations within its territory.[36] Thus, while states may criminalize conduct that occurs wholly outside their borders,[37] the system as a whole is stable because states do not directly exercise law enforcement functions in other countries without first obtaining consent.[38]

In a similar vein, scholarship interrogating the extraterritorial aspects of law enforcement surveillance on the Internet has focused on the extraterritori-

34. *See, e.g.*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (AM. LAW INST. 1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.").

35. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD 156-58 (2006); Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 45-47; Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1205-13 (1998).

36. *See* Goldsmith, *supra* note 35, at 1220-21 (arguing that the "threat of multiple regulation of cyberspace information flows" must be "measured by a regulation's enforceable scope," which is limited to persons and entities with presence or assets in the territory of the regulating state).

37. As a matter of domestic law, Congress could in principle extend the reach of the criminal law as far as it likes, subject to constitutional limits. *See* John H. Knox, *A Presumption Against Extrajurisdictionality*, 104 AM. J. INT'L L. 351, 351 (2010). The Supreme Court has never clarified whether such limits exist. *See id.*; *cf.* Lea Brilmayer & Charles Norchi, *Federal Extraterritoriality and Fifth Amendment Due Process*, 105 HARV. L. REV. 1217, 1223 (1992) (arguing that constitutional due process "limits extraterritorial application of substantive federal law").

38. *See, e.g.*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2); ROBERT CRYER ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE § 3.2.3, at 44 (2d ed. 2010) (defining "enforcement" (or "executive") jurisdiction as "the right to effect legal process coercively, such as to arrest someone, or undertake searches and seizures"); *see also* Alvarez-Machain v. United States, 331 F.3d 604, 625 (9th Cir. 2003) (en banc) ("Extraterritorial *application* [of a criminal statute], in other words, does not automatically give rise to extraterritorial *enforcement* authority."), *rev'd on other grounds sub nom.* Sosa v. Alvarez-Machain, 542 U.S. 692 (2004).

al scope of Fourth Amendment rights.[39] It lacks a thorough treatment of the interstate jurisdictional frictions that result and the implications such conduct might have on our conceptions of sovereignty, foreign relations, and Internet governance.

At the other end of the spectrum, the threat of harmful cross-border cyberoperations has become ever-present and raises questions about the capacity of states to protect their sovereign interests in territorial cyberinfrastructure.[40] There is a scholarly consensus that in theory, a cross-border cyberoperation could be characterized as an "internationally wrongful act" (permitting a state to respond with countermeasures under customary international law), a prohibited "use of force" (authorizing otherwise prohibited force in self-defense), or an "armed attack" (entitling harmed states to use otherwise prohibited force in self-defense), depending on the scope and severity of the damage caused by the operation.[41] States also use their domestic computer crime laws to criminalize cross-border cyberoperations by both state and nonstate actors that have effects in their territory.[42]

---

39. *See, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 380-87 (2015) (arguing that Fourth Amendment territoriality is a poor fit for regulating government collection of electronic data and discussing alternatives); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 304-08 (2015) (arguing that virtual contacts alone are insufficient to create Fourth Amendment rights for foreign-located persons absent physical contacts or a legal relationship with the United States).

40. *See* Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV 1503, 1507 & n.19 (2013) (noting that "[v]irtually all legal scholarship approaches cyber-security from the standpoint of the criminal law or the law of armed conflict" and collecting the leading scholarship on both perspectives).

41. *See, e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 36, 42-43, 45, 54 (Michael N. Schmitt ed., 2013) (presenting a nonbinding formulation of the international law norms applicable to cyberwarfare, unanimously agreed upon by a group of international experts brought together by the NATO Cooperative Cyber Defence Centre of Excellence); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 839-57 (2012) (discussing the challenges of obtaining a consensus as to how an individual cyberattack *should* be classified despite the consensus that cyberattacks *could* be classified as a prohibited "internationally wrongful act," "use of force," or "armed attack"). For an extensive discussion of the debate surrounding the definition of "force" and "armed attack" in Articles 2(4) and 51 of the U.N. Charter, see Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 431-37 (2011).

42. In 2002, for example, Russian authorities charged an FBI agent with violating hacking and espionage laws by logging into a secure computer located in Russia and collecting data. *See* Mike Brunker, *FBI Agent Charged with Hacking*, NBC NEWS (Aug. 15, 2002), http://www.nbcnews.com/id/3078784. The FBI obtained log-on credentials from Russian hackers who were lured into the United States as part of an elaborate sting operation. *Id.* More recently, in 2014 U.S. authorities charged members of the Chinese military under U.S. economic espionage laws for exfiltration of intellectual property data from U.S. corporations. *See* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor

footnote continued on next page

To be sure, the FBI's existing hacking techniques, properly executed, do not rise to the level of a cyber "armed attack," which would permit a state to respond with force under Article 51 of the U.N. Charter.[43] Nor is there an absolute prohibition on cross-border cyberoperations as a matter of international law.[44] But the scope of harm a cross-border cyberoperation might cause varies, as does interpretation of existing international norms.[45] Indeed, "[p]recisely when a non-consensual cyber operation violates the sovereignty of another State is a question . . . that ultimately will be resolved through the practice and opinio juris of States."[46] As such, the United States has an interest in leading the effort to clarify existing international norms as applied to government hacking and the development of norms through diplomatic measures.[47]

These circumstances highlight the failure of the existing rules to regulate the use of network investigative techniques. Rank-and-file law enforcement officials[48] have discretion over which crimes trigger the use of hacking techniques, the range of techniques that may be used once a warrant authorizes a search, and the ability to target computers of nonsuspects. Because the legal process governed by Rule 41 presumes that targets are territorially located, it does not consider the risk of potentially significant foreign relations consequences or encourage law enforcement to engage with foreign relations or national security experts in other parts of government.

This Article is the first to consider the cross-border implications of the use of network investigative techniques to pursue targets on the dark web and the institutional design problems that result. Broadly, it asks whether (and how) the legal architecture of cross-border investigations should adapt to the dark web, a space that defies our conceptions of geography and identity, and a reality where investigative activities for everyday crimes have a heightened

Organization for Commercial Advantage (May 19, 2014), http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

43. U.N. Charter art. 51. Forceful responses to hostilities below the threshold of an "armed attack" are only permissible with U.N. Security Council authorization. Specifically, Article 41 authorizes the Security Council to take measures that do not involve armed force, whereas Article 42 authorizes the Security Council to escalate measures to the use of armed force in the event nonforceful measures are inadequate. *See id.* arts. 41-42.

44. Brian J. Egan, Legal Advisor, U.S. Dep't of State, Remarks on International Law and Stability in Cyberspace, Address at Berkeley Law School (Nov. 10, 2016), https://www.law.berkeley.edu/wp-content/uploads/2016/12/egan-talk-transcript-111016.pdf.

45. *See infra* Part II.C.5.

46. Egan, *supra* note 44.

47. *Id.*

48. By "rank-and-file," this Article means "frontline agents who interface with the public." *See* John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205, 210 (2015).

extraterritorial—and thus foreign relations—impact. More narrowly, it contends that extraterritorial aspects of network investigative techniques demonstrate the need for new substantive and procedural regulations that balance law enforcement goals with countervailing foreign relations interests.

This Article then identifies the failures of the existing legal process, suggests a number of substantive policy preferences that the executive branch should implement in response, and lays out a regulatory scheme for their implementation and enforcement that involves "a complex, dynamic interaction of institutions that simultaneously work together, challenge each other, defend themselves and divide responsibility."[49] While the judiciary's checks will remain essential to the implementation and enforcement of network investigative techniques, self-regulation within the executive branch and regulation from Congress are needed to produce decisions that are reliable, legitimate, and in the public interest.

This Article proceeds in three Parts. Part I describes how existing surveillance methods fail to solve crimes on the dark web and how the hacking techniques police use in response will unavoidably result in cross-border cyberexfiltration operations. Part II turns from the facts to the governing law, focusing on how the rules of criminal procedure limit the exercise of existing law enforcement functions to the territorial United States but fail to function in the same way when applied to network investigative techniques on the dark web. Cross-border cyberexfiltration operations are in obvious tension with international norms and thus raise a variety of foreign relations risks. Part III evaluates the shortcomings of the existing legal process and argues that a new regulatory framework is needed to govern network investigative techniques. It also offers initial thoughts as to what the new rules might look like and which institutions should set, implement, and enforce them.

Importantly, this Article does not attempt to resolve every issue prompted by the dark web or hacking techniques. Nor does it attempt to resolve the issue how states should regulate cross-border cyberoperations. Instead, it is intended to offer a policymaking framework for this new surveillance technology that minimizes immediate foreign relations and national security risks and allocates the authority to make new decisions on appropriate procedures to the institutions most competent to address them. To that end, the ultimate question is not how well the status quo functions but rather whether adjustments may produce better foreign relations outcomes without sacrificing law enforcement's ability to identify and locate criminal suspects that have taken cover on the dark web.

---

49. *See* Edward L. Rubin, *Institutional Analysis and the New Legal Process*, 1995 WIS. L. REV. 463, 467 (book review).

I. Law Enforcement in the Dark

A. The Dark Web

The dark web is a private global computer network that enables users to conduct anonymous transactions without revealing any trace of their location. One such private network, whose characteristics I will use as a model for my analysis, is the Tor Network.[50] Computers on the Tor Network use an encrypted communications protocol that cannot be accessed using normal web browsers. Instead, they require the use of special software, like the Tor Browser. Proper use of the Tor Network makes it practically impossible for governments to trace the location of computers hosting "hidden" websites on the network, the location of computers accessing those hidden websites, or the location of computers that tunnel through the network to "anonymously" visit public websites on the World Wide Web.[51]

The Tor Network protects its users from two types of surveillance. First, it protects users from a common form of surveillance called "traffic analysis," which is the real-time interception and examination of communications in order to deduce information.[52] Second, it prevents governments from using communications "metadata"—information *about* a communication, such as its source, destination, and size—acquired from third-party service providers to draw conclusions about the communicators and their behavior.[53]

---

50. The terms "dark web" and "Tor Network" are used interchangeably throughout this Article. The Tor Network was originally developed by the U.S. military and is now open source and publicly funded. *See generally* KRISTIN FINKLEA, CONG. RESEARCH SERV., R44101, DARK WEB 3 (2015); *Tor: Sponsors*, TOR PROJECT, https://www.torproject.org/about/sponsors.html.en (last visited Apr. 4, 2017) (listing past and present contributors to the Tor Network).

51. An "overlay network" is a computer network that is built on top of another network. Computers in the overlay network can be thought of as being connected by virtual or logical links, each of which corresponds to a path that often runs through many physical links, in the underlying physical network. Examples of overlay network deployments include virtual private networks, peer-to-peer networks such as Napster and BitTorrent, and Voice over Internet Protocol (VoIP) services such as Skype. *See* Guillermo Agustín Ibáñez Fernández, *New Computer Network Paradigms and Virtual Organizations*, *in* 2 GORAN D. PUTNIK & MARIA MANUELA CUNHA, ENCYCLOPEDIA OF NETWORKED AND VIRTUAL ORGANIZATIONS 1066, 1073 (2008); *see also* 2 IN LEE, HANDBOOK OF RESEARCH ON TELECOMMUNICATIONS PLANNING AND MANAGEMENT FOR BUSINESS 871 & tbl.2 (2009) (referring to overlay network deployments); Roger Dingledine et al., Tor: The Second-Generation Onion Router (n.d.), https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

52. *See* Stephen Northcutt, *Traffic Analysis*, SANS TECH. INST. (May 16, 2007), http://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis.

53. *See* Tony Gill, *Metadata and the Web*, *in* INTRODUCTION TO METADATA 20, 22 (Murtha Baca ed., 2d ed. 2008) (defining "metadata" as "a structured description of the essential attributes of an information object" (italics omitted)); David Talbot, *Dissent Made Safer:*

footnote continued on next page

As a technical matter, the Tor Network protects users' communications from government surveillance because it disassociates communications "metadata" from communications "content" and bounces message packets off several intermediate computers, or "proxies," before steering them to their originally intended destination.[54] Proxy computers are scattered around the globe, provided by people who have volunteered their computers to the anonymity network.[55]

As a practical matter, the Tor Network can protect user communications from traffic analysis in two ways. First, users can "tunnel" through the Tor Network when communicating with publicly accessible webpages on the World Wide Web. As a result, when a user tunnels through the Tor Network in order to browse a webpage, her Internet traffic appears to originate at a proxy computer rather than at her true connection. Conversely, from the perspective of an ISP, traffic from the user's computer appears to be heading to another proxy computer rather than to the actual intended destination.

Thus, someone located in Seattle who has anonymized his communications using a series of proxies, the last of which is located in Italy, will appear to the destination webpage to be a user in Italy. Likewise, someone in Iran who has run his communications through a series of proxies, the last of which is located in San Francisco, will appear to the destination website as a web surfer from San Francisco and to the local ISP in Iran as though he were attempting to communicate with a proxy computer.

The second way people can use the Tor Network to protect their communications is through the Tor Network's hidden services feature, which allows people to host content or services without exposing the physical location of their servers. Hidden services are only accessible by those who use software

How Anonymity Technology Could Save Free Speech on the Internet, MIT TECH. REV. (Apr. 21, 2009), https://www.technologyreview.com/s/413091/dissent-made-safer ("In the United States, for example, libraries and employers often block content, and people's Web habits can be—and are—recorded for marketing purposes by Internet service providers (ISPs) and by the sites themselves.").

54. The Tor Network is currently maintained by the Tor Project, a 501(c)(3) nonprofit based in the United States and funded partly by a number of federal grants from the U.S. government. *See* Natascha Divac & Sam Schechner, *Munich Attack Investigation Shines Light on 'Dark Web,'* WALL ST. J. (July 26, 2016, 9:03 PM ET), https://www.wsj.com/articles/before-the-shootings-munich-gunman-visited-the-dark-web-1469558210; Damian Paletta, *How the U.S. Fights Encryption—and Also Helps Develop It*, WALL ST. J. (Feb. 22, 2016, 12:31 AM ET), http://www.wsj.com/articles/how-the-u-s-fights-encryptionand-also-helps-develop-it-1456109096; *see also Tor: Sponsors*, *supra* note 50.

55. *See* FINKLEA, *supra* note 50, at 3-4, 4 n.20. As discussed in Part II.A below, foreign-located proxy computers are out of reach of U.S. subpoena authority unless their owners fall under the personal jurisdiction of U.S. courts (for instance, due to nationality or territorial presence).

that enables them to get on the Tor Network, and even then, communications between a hidden service (such as the Silk Road) and its users occur though a "rendezvous point," a proxy that provides an additional layer of protection from traffic analysis.

Civil liberties advocates promote the use of the Tor Network to maintain free speech, privacy, and anonymity. For example, the Tor Network may be used to circumvent government censorship, enabling users to access online destinations that have been blocked by authoritarian regimes.[56] The Tor Network can also be used to facilitate spaces online where individuals can conduct sensitive communications without fear of being tracked. For example, individuals may want to anonymize their communications to research sensitive issues such as physical or mental illness or to engage in political dissent without government detection. Businesses may want to use the Tor Network to prevent corporate spies from gaining any competitive advantage by learning whom their employees are communicating with or what topics they are researching.

The added protection of the "hidden services" feature can also be used to circumvent a common censorship technique used by repressive regimes where websites deemed unfit for public consumption (such as blogs that promote dissent) are taken down and their web administrators arrested.[57] Journalists and whistleblower groups also use the Tor Network's hidden services feature to communicate with sources. For example, SecureDrop, an open source whistleblower submission system initially created for the *New Yorker*, can be

56. Some governments have responded by enacting regulations around the use of the Tor Network or blocking access to known proxy nodes in the Tor Network. *See, e.g.*, Lorenzo Franceschi-Bicchierai, *Turkey Doubles Down on Censorship with Block on VPNs, Tor*, MOTHERBOARD (Nov. 4, 2016, 2:20 PM), http://motherboard.vice.com/read/turkey-doubles-down-on-censorship-with-block-on-vpns-tor. This, in turn, has led to the development of "bridge relay" technology that enables the user to gain access to the Tor Network by accessing Tor relays that are not listed in the main Tor directory (and thus are unknown to government censors). *See Tor: Bridges*, TOR PROJECT, https://www.torproject.org/docs/bridges (last visited Apr. 4, 2017).

57. If government agents are unable to locate the server hosting the blog, they cannot physically take it down (in the event it is located in-country) or request that a third party (or another country) do so. *See infra* Part I.B. Facebook set up a hidden services account in 2012. *See* Andy Greenberg, *Why Facebook Launched Its Own 'Dark Web' Site*, WIRED (Oct. 31, 2014, 12:31 PM), https://www.wired.com/2014/10/facebook-tor-dark-site ("[N]o surveillance system watching either Facebook's connection or the user's local traffic should be able to match up a user's identity with their Facebook activity."); Alec Muffett, *Making Connections to Facebook More Secure*, FACEBOOK (Oct. 31, 2014, 4:30 AM), https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237.

used by media organizations to securely accept documents from and communicate with anonymous sources.[58]

Not surprisingly, criminals and other malicious actors flocked to the dark web for its promise of an anonymous and secure platform for "conversation, coordination, and action."[59] Modern criminals use the dark web to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft.[60] Platforms like the Silk Road provide a means for existing brick-and-mortar criminals to globalize their operations with virtual impunity. Increasingly, criminals use the dark web to facilitate crimes traditionally conducted in the physical world, such as currency counterfeiting,[61] drug distribution,[62] child exploitation,[63] human trafficking,[64] arms and ammunition sales,[65] assassination,[66] and terrorism.[67]

B. Failure of Conventional Surveillance Methods

According to the DOJ, use of the dark web by criminals to anonymize communications makes it "impossible for law enforcement" to pursue criminal suspects.[68] In computer crime cases, locating the computer used by the perpetrator is the most critical step in discovering the perpetrator's identity

58. Tom Lowenthal & Geoffrey King, *How SecureDrop Helps CPJ Protect Journalists*, COMMITTEE TO PROTECT JOURNALISTS (May 12, 2016, 7:00 AM), https://cpj.org/x/686d; *see* Lorenzo Franceschi-Bicchierai, *SecureDrop: Aaron Swartz's Platform for Whistleblowers Rebooted*, MASHABLE (Oct. 15, 2013), http://mashable.com/2013/10/15/secure-drop-aaron-swartz-freedom-of-the-press-foundation/#.Tu9ZMRgqkqm.

59. *See* FINKLEA, *supra* note 50, at 8.

60. *See id.* at 8-10 (describing ways in which the dark web facilitates criminal activity).

61. Press Release, U.S. Dep't of Justice, Four Charged in International Uganda-Based Cyber Counterfeiting Scheme (Apr. 2, 2015), https://www.justice.gov/opa/pr/four-charged-international-uganda-based-cyber-counterfeiting-scheme.

62. Press Release, U.S. Att'y's Office for the S. Dist. of N.Y., *supra* note 1.

63. GOODMAN, *supra* note 1, at 206.

64. *Id.* at 207-08.

65. *Id.* at 205-06.

66. *Id.* at 206; *see* Andy Greenberg, *Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins*, FORBES (Nov. 18, 2013, 8:30 AM), http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/#2277df031ac1.

67. According to German authorities, eighteen-year-old gunman Ali David Sonboly likely bought his handgun—which he used to kill nine people and himself in Munich on July 22, 2016—illegally on the dark web. Ruth Bender & Christopher Alessi, *Munich Shooter Likely Bought Reactivated Pistol on Dark Net*, WALL ST. J. (July 24, 2016, 4:23 PM ET), http://www.wsj.com/articles/munich-shooter-bought-recommissioned-pistol-on-dark-net-1469366686.

68. Letter from Mythili Raman to Judge Reena Raggi, *supra* note 25, at 2.

and collecting evidence to build a successful prosecution.[69] Without the perpetrator's laptop, investigators will lack evidence attributing virtual criminal conduct to an actual person.[70]

Conventional investigative methods rely on collection of data from third parties through compulsion and consent. When digital evidence is controlled by a person or entity subject to U.S. personal jurisdiction, compulsory process is used to obtain digital evidence. When digital evidence is outside U.S. jurisdiction—such as when it is controlled by an entity with no physical presence or assets in the United States—formal and informal law enforcement cooperation mechanisms are used to obtain it.

Investigators typically begin a computer crime investigation with nondescript information about the perpetrator's online alias, such as the e-mail address used to transmit communications.[71] Investigators may then decide to request all account information associated with the e-mail address from the third-party e-mail provider. In the event the e-mail service provider is beyond U.S. jurisdiction, the investigators will likely initiate protocols to use diplomatic channels to request that the host country provide the evidence. Before the advent of the dark web, the third-party disclosure would yield "true" identifying information—such as an Internet Protocol (IP) address registered with the ISP[72]—from which investigators could infer the user's log-on location.[73] Once the location of the device was determined, investigators could apply for a warrant to physically seize the device and extract its contents.[74]

69. *Cf.* Michael B. Mukasey, The Attorney General's Guidelines for Domestic FBI Operations 7 (2008), http://www.usdoj.gov/ag/readingroom/guidelines.pdf ("In most ordinary criminal investigations, the immediate objectives include . . . identifying, locating, and apprehending the perpetrators . . . .").

70. *See* 3 PETER W. GREENWOOD ET AL., NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, R-1778-DOJ, THE CRIMINAL INVESTIGATION PROCESS: OBSERVATIONS AND ANALYSIS 65 (1975), https://www.ncjrs.gov/pdffiles1/Digitization/148118NCJRS.pdf (defining a "solved" case as one where investigators know "the identity of the perpetrator(s), even if additional work [is] needed to locate the perpetrators or to establish the facts needed to prove guilt in court").

71. *See, e.g.*, Sanders Affidavit, *supra* note 17, ¶¶ 5-6, 11 (listing nondescript e-mail addresses used to communicate threatening messages to a school).

72. *Cf.* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 284 (2005) ("In most cases, the biggest investigative lead comes in the form of an originating Internet Protocol (IP) address recorded by the bank's servers.").

73. *Cf.* Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 912-13 (2011) (describing various technologies that enable IP geolocation).

74. *See* Kerr, *supra* note 72, at 285 ("The process of collecting electronic evidence in computer hacking cases generally divides into three steps. It begins with the collection of stored evidence from third-party servers, turns next to prospective surveillance, and ends with the forensic investigation of the suspect's computer.").

Increasingly, digital evidence is beyond U.S. jurisdiction. When evidence is *not* in the custody or control of a party that falls under U.S. jurisdiction, investigators use *consent-based* cross-border evidence collection methods, implemented through a series of formal and informal relationships.[75] The principal and least controversial tool for evidence collection in such cases is a Mutual Legal Assistance Treaty (MLAT).[76] MLATs facilitate law enforcement cooperation and assistance in support of ongoing criminal investigations or proceedings.[77] MLATs generally contain provisions for locating and identifying persons and items, serving process, executing search warrants, taking witness depositions, summoning witnesses; and seizing assets.[78]

MLATs are negotiated by the U.S. Department of State[79] and implemented by the DOJ's Office of International Affairs (OIA), the DOJ's foreign relations office.[80] Once the agreement goes into force, the OIA is the "[c]entral [a]uthority" tasked with working with "foreign counterparts to ensure effective treaty implementation."[81] The OIA also serves an interdepartment coordination role, briefing "the Attorney General and other senior [DOJ] officials on international issues and provid[ing] advice on sensitive law enforcement matters that could impact the foreign relations and strategic interests of the United States."[82]

In addition to formal diplomatic mechanisms, federal law enforcement actors exchange criminal investigation-related information through informal channels and relationships cultivated to facilitate interstate law enforcement cooperation and access to evidence.[83] The United States also engages in joint investigations, which are coordinated investigative efforts among law enforcement agencies of different countries in criminal matters.[84]

---

75. In the past, the use of network investigative techniques overseas has relied on consent-based mechanisms. *See infra* note 115 and accompanying text.

76. *See* 7 U.S. DEP'T OF STATE, FOREIGN AFFAIRS MANUAL § 962.1 (2013) (providing a brief historical overview of MLATs and a list of bilateral MLATs in force).

77. *See id.* § 962.1(a).

78. *See id.*

79. *See id.* § 962.1.

80. *See Frequently Asked Questions Regarding Evidence Located Abroad*, U.S. DEP'T JUST., http://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-evidence-located-abroad (last updated June 11, 2015).

81. *Office of International Affairs (OIA)*, U.S. DEP'T JUST., https://www.justice.gov/criminal-oia (last visited Apr. 4, 2017).

82. *Id.*

83. *See Frequently Asked Questions Regarding Evidence Located Abroad*, *supra* note 80.

84. *See, e.g.*, United States v. Emmanuel, 565 F.3d 1324, 1328, 1330 (11th Cir. 2009); *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 159-60 (2d Cir. 2008); United States v. Barona, 56 F.3d 1087, 1089-93 (9th Cir. 1995); United States v. Behety, 32 F.3d 503, 510-11 (11th Cir. 1994); United States v. Marzook, 435 F. Supp. 2d 708, 775-

footnote continued on next page

Consider an elementary school that receives a series of bomb threats by e-mail.[85] The perpetrator uses a nondescript e-mail address and leaves no clues that can be used to discover his true identity.[86] Instead, investigators must follow the digital trail the perpetrator's computer has laid out. Investigators will likely first subpoena the e-mail service provider whose services were used to communicate the threat, requesting disclosure of evidence associated with the perpetrator's account.[87] If the ISP does not fall under U.S. jurisdiction—for example, if it is located in Italy—investigators will use formal and informal mechanisms to seek assistance from cooperating agencies abroad. Investigators may pursue formal procedures, calling the OIA and triggering the MLAT protocols in Italy. The lead investigator may also use informal channels, such as his personal relationships with foreign law enforcement authorities. Either way, the ISP's disclosure will likely include an IP "address log" detailing the activity history for the e-mail address.[88]

Use of the dark web by the perpetrator, however, renders these conventional evidence collection methods obsolete. Recall that when someone tunnels though the dark web to browse a public webpage, his Internet traffic appears to originate from one of thousands of "proxy" computers rather than the one he is using.[89] Without the ability to obtain a true location for the targeted device, investigators are unable to initiate conventional evidence collection protocols.

---

77 (N.D. Ill. 2006); United States v. Castro, 175 F. Supp. 2d 129, 132-33 (D.P.R. 2001); *cf.* ORGANISATION FOR ECON. CO-OPERATION & DEV., TYPOLOGY ON MUTUAL LEGAL ASSISTANCE IN FOREIGN BRIBERY CASES 51 (2012), http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf (describing "Joint Investigative Teams," which are used by European Union member countries and allow "two or more countries to form a team to conduct a single criminal investigation").

85. This hypothetical is loosely based on a case from 2007. *See* Sanders Affidavit, *supra* note 17, ¶ 11.

86. *Cf. id.* ¶ 6.

87. *See* 18 U.S.C. § 2703(c)(2) (2015) (requiring third-party ISPs to disclose user account information with a subpoena).

88. If the ISP keeps comprehensive records, additional information such as a billing address may also be disclosed. *Id.*; *see* Kerr, *supra* note 72, at 286 n.11 (citing United States v. Kennedy, 81 F. Supp. 2d 1103, 1107 (D. Kan. 2000), as an example of a case where the customer's billing address and telephone number were disclosed). Once a suspect is identified, investigators and prosecutors decide whether there is sufficient evidence to bring a successful prosecution. *See* Kerr, *supra* note 72, at 289. The suspect's true identity opens up the door to all sorts of evidence and investigation methods. This may include indirect collection of digital evidence (for instance, in the form of e-mails, GPS, and telephony data) from third parties through compelled disclosure. *See* 18 U.S.C. §§ 2701-2711; *see also infra* Part II.A. This may also include direct collection, authorized by warrant, in the form of physical surveillance methods or collection of digital evidence from the device used to perpetrate the crime. *See infra* Part II.B.

89. *See supra* Part I.A.

In the dark web version of our hypothetical, the suspect tunnels though the dark web to anonymize a connection to a third-party e-mail service provider. Thus, surveillance methods that depend on disclosures from third-party ISPs can no longer be used to locate investigation targets.[90] Investigators are still authorized to subpoena the e-mail provider for relevant account information. However, this time, the third-party disclosures reveal to investigators *only* that the suspect anonymized his communications.[91] The investigators are unable to physically seize the computer, whether through direct means or with the cooperation of another country. With no other leads, the investigation grinds to a halt.[92]

Use of the dark web by criminal actors enables secret, untraceable criminal activity to take place at scale.[93] The existence of hidden services like the Silk Road "dramatically lower[s] the entry barriers into the underground

90. *See* Kerr, *supra* note 72, at 286.

91. The investigators know this because the IP address received is that of a known "proxy" computer. When someone using the Tor Network browses a webpage, his Internet traffic appears to originate from one of hundreds of Tor's exit nodes rather than his home connection, and the communication cannot be traced backwards. Conversely, from the perspective of an ISP on the originating end, traffic from the Tor user appears to be heading toward one of hundreds of Tor's entry nodes rather than the actual intended destination. As a result, law enforcement can no longer use third-party disclosures to identify a target. *See generally* FINKLEA, *supra* note 50, at 3-5.

92. Notably, in all publicly available warrant applications reviewed by the Author, the application affiant has asserted that locating the true IP address of the perpetrator is impossible but for the use of network investigative techniques. For example, one affidavit stated:

> Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple other computers or "nodes," . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

Affidavit of Special Agent Douglas Macfarlane in Support of Application for Search Warrant ¶ 31, *In re* Search of Computs. That Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015); *see also* United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *5-6 (N.D. Okla. Apr. 25, 2016) ("The critical point is that without the use of such techniques as [network investigative techniques], agents seeking to track a Tor user to his home computer will not be able to take that pursuit beyond the exit node from which the Tor user accessed the regular Internet."), *report and recommendation adopted by* 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

93. It is perhaps for this reason that the FBI considers computer crimes to be "the most significant crimes confronting the United States." FINKLEA, *supra* note 50, at 9; *see also* James B. Comey, Dir., FBI, The FBI and the Private Sector: Closing the Gap in Cyber Security, Remarks at the RSA Cyber Security Conference (Feb. 26, 2014), https://www.fbi.gov/news/speeches/the-fbi-and-the-private-sector-closing-the-gap-in-cyber-security ("Before he left, Director Mueller told me that he believed cyber issues would come to dominate my tenure as counterterrorism had dominated his time as Director. And I believe he is right. We must be agile and predictive on every front. And we must use every tool and authority at our disposal to stop these malicious activities.").

economy—for both buyers and sellers alike."[94] The resurgence of several underground marketplaces in the wake of the Silk Road shutdown underscores the asymmetry between investigators' ability to track unlawful activity and criminals' capacity to commit crimes on the dark web.[95]

C. Hacking as an Investigative Tool on the Dark Web

Anonymity tools are not the first technological change to leapfrog law enforcement surveillance capabilities.[96] The FBI has termed this leapfrog phenomenon "going dark."[97] In the 1990s, for instance, law enforcement lost its ability to wiretap calls when telephone companies switched from copper cables to digital telephony.[98] The result was the passage of the Communications Assistance for Law Enforcement Act in 1994, which required telephone carriers to install standardized equipment so they could assist police with electronic wiretaps.[99] However, such "backdoor" solutions are not technologically feasible on the dark web due to its decentralized architecture, use of open software, and core functionality requirements.[100]

Network investigative techniques circumvent the challenges the dark web poses by using the Internet to facilitate the delivery and installation of surveillance software (malware[101]) on the target device.[102] Formerly, an

94. Government Sentencing Submission, *supra* note 15, at 2.

95. *See id.* at 3, 13; Press Release, Sen. Tom Carper, *supra* note 14.

96. Bellovin et al., *supra* note 18, at 8-18 (providing a history of communications technologies leapfrogging law enforcement capabilities, including cellular telephony, VoIP, and end-to-end encryption). *See generally* William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795, 1804 (1998) (noting that criminals generally have an incentive to change patterns once law enforcement agencies adapt).

97. *Going Dark*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/operational-technology/going-dark (last visited Apr. 4, 2017) (describing the "going dark" issue as the FBI's inability to access evidence due to technological barriers).

98. Bellovin et al., *supra* note 18, at 7 (noting that with the advent of digital telephony it was no longer possible to tap lines with the traditional method of "two alligator clips and a tape recorder").

99. *See id.* at 6-7; *see also* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 103, 108 Stat. 4279, 4280-82 (1994) (codified as amended at 47 U.S.C. § 1002 (2015)).

100. Bellovin et al., *supra* note 18, at 6-7, 18. A thorough discussion of how the open, distributed architecture of certain anonymity tools makes technological backdoors infeasible is beyond the scope of this Article. For our purposes, it is sufficient to know that (1) distributing a technology's network architecture may place its components beyond a state's jurisdictional reach and (2) using open architecture allows transferability of components by independent third parties.

101. *See supra* note 17.

102. *See* Memorandum from Sara Sun Beale & Nancy King to Advisory Comm. on Rules of Criminal Procedure, *supra* note 32, at 2 (describing network investigative techniques as

footnote continued on next page

investigator wishing to search a computer using conventional methods had to gain access to the physical location of the computer and generate a copy of its hard drive. This requires knowledge of the computer's physical location, which the dark web obscures.

Network investigative techniques create a way for investigators to reach a computer that does not require knowledge of its physical location. Rather than traversing "physical" pathways—such as roads and bridges—to reach the target's physical address, investigators deploy malware that traverses "virtual" pathways—such as connections between computers and bridges between networks—to reach the computer's virtual IP address. Importantly, the new methods can reach the same destination.[103] Once malware penetrates the target, it converts the computer into a surveillance device.

Network investigative techniques function in two steps: access to data and extraction of data.[104] The "access" step can be thought of as arriving at the location of a file cabinet and picking its lock,[105] and the "extraction" step can be thought of as rifling through the file cabinet's contents.[106]

"remote access searches, in which the government seeks to obtain access to electronic information or an electronic storage device by sending surveillance software over the Internet").

103. A physical search requires knowing the *physical* location of a target computer. By contrast, a remote search requires a means to communicate with the target computer, such as an active e-mail address. *See infra* notes 107-12 and accompanying text.

104. Description and analysis of predeployment and postexecution steps are beyond the scope of this Article. Of course, there are important steps that occur before deployment, such as vulnerability harvesting (analogized to gaining knowledge about the various types of locks that are in use by file cabinet makers and how to unlock them) and target reconnaissance (analogized to figuring out what types of locks a particular target uses and whether the attacker can access them). *See generally* Bellovin et al., *supra* note 18, at 34-41.

105. The "access" step requires two critical pieces of information: (1) the existence of a software vulnerability and (2) an available path or "attack vector" to successfully access and exploit that vulnerability. *Cf.* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 83 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT] ("Access would be an available path for reaching the file cabinet . . . ."). A vulnerability can be analogized to a faulty lock on the file cabinet. It is a security flaw or weakness that can be used by an attacker to compromise the system. A vulnerability can be (1) a code-based vulnerability, such as a weakness in the browser application used by the target; (2) a human vulnerability, where the weakness is a human who possesses credentials needed to access a system; or (3) a combination of the two, where a human vulnerability enables the attacker to deceive the user into performing an act that would (indirectly) cause the system to be compromised. At any rate, the relevant state action for the "access" step of our analysis is the execution of the attack vector to access and exploit a particular software or hardware vulnerability.

106. *Id.* ("The payload is the action taken by the intruder after the lock is picked.").

In the access step, law enforcement deploys malware that travels across the Internet to the target device, where it exploits a software security vulnerability that enables access to the system.[107] As in the physical world, an investigator may take one of many different paths in cyberspace to reach the location of a target. To that end, deployment mechanisms divide into three categories: spear phishing attacks, watering hole operations, and man-in-the-middle attacks. In a "spear phishing" operation, law enforcement targets an individual device by sending the target a communication (typically through e-mail or social media) to convince her to take a particular action—such as clicking on a link or opening an attachment—that triggers the delivery of malware.[108] In a "watering hole" operation, investigators first gain control of a server and then use it to distribute attacks to all visitors.[109] And in a "man-in-the-middle" attack, investigators lodge themselves between two endpoints of a communication so they can secretly relay or alter communications between parties.[110]

In the extraction step, a set of malware instructions known as a "payload" is executed on the device, effectively turning it into a surveillance tool.[111] Once installed, malware can cause a computer to perform any task the computer is capable of performing. For example, it may direct files and communications to a server controlled by law enforcement or gather images and sound at any time

---

107. *See id.* at 86-87; Bellovin et al., *supra* note 18, at 25-26.

108. *See* Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J. (Aug. 3, 2013, 3:17 PM ET), http://on.wsj.com/14mj2pV (noting that investigators "us[e] a document or link that loads software when the [targeted] person clicks or views it"); *cf.* Tom N. Jagatic et al., *Social Phishing*, COMM. ACM, Oct. 2007, at 94, 94, 96 (demonstrating empirically that phishing attacks impersonating a friend of the target are more successful than those in which the sender is not known to the target).

109. *See, e.g.*, Darien Kindlund, *Holiday Watering Hole Attack Proves Difficult to Detect and Defend Against*, ISSA J., Feb. 2013, at 10, 11 (describing a watering hole attack that infected visitors of a certain page on the website of the Council of Foreign Relations); Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, WASH. POST (Jan. 21, 2016), http://wpo.st/nom72 (describing the use of watering hole attacks used to hack computers that visit hidden child pornography sites).

110. Bellovin and his coauthors describe a man-in-the-middle attack as follows:

> A Man-in-the-Middle attack is a method of gaining access to target information in which an active attacker interrupts the connection between the target and another resource and surreptitiously inserts itself as an intermediary. This is typically done between a target and a trusted resource, such as a bank or email server. To the target the attacker pretends to be the bank, while to the bank the attacker pretends to be the target. Any authentication credentials required (e.g., passwords or certificates) are spoofed by the attacker, so that each side believes they are communicating with the other. But because all communications are being transmitted through the attacker, the attacker is able to read and modify any messages it wishes to.

Bellovin et al., *supra* note 18, at 24 (bolding omitted).

111. *See* NRC REPORT, *supra* note 105, at 88.

the executing agent chooses.[112] From behind a screen at the other end of the connection, investigators are able to deploy immensely powerful techniques that scale with ease to track and surveil suspects.

But consider this important wrinkle: the clear majority of dark web users are *outside* the territorial United States.[113] And because each computer's location is theoretically indistinguishable from the next, any law enforcement target pursued on the dark web may be located overseas.[114]

The overseas cyberexfiltration operations that result from the use of network investigative techniques are a significant change in the way U.S. law enforcement engages in cross-border investigations. Before the amendment to Rule 41, criminal legal process authorized methods for evidence collection that aligned with customary international law, where it is considered an incursion on another state's sovereignty to carry out law enforcement functions within another state without that state's consent. To that end, law enforcement agencies relied on the United States' diplomatic relations and treaties with other countries, seeking permission from the host state before deploying personnel and requesting assistance from local authorities to collect foreign-located evidence when possible. For instance, the Drug Enforcement Administration has recently confirmed that it has used hacking tools on seventeen devices in a foreign country pursuant to a foreign court order and with the cooperation of foreign officials.[115]

In contrast to conventional methods, the exercise of extraterritorial law enforcement functions will be unilateral. It will not be limited to matters of national security, nor will it be coordinated with the State Department or other relevant agencies.[116] Case-by-case investigatory decisions made by rank-and-file officials[117] will have direct overseas consequences. The foreign

112. *See In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 755-56, 761 (S.D. Tex. 2013) (denying on territorial limitation grounds an application for a warrant to use network investigative techniques that control the computer's camera and calculate the latitude and longitude of the device); *see also* Timberg & Nakashima, *supra* note 18 (describing features of network investigative techniques).

113. *See Top-10 Countries by Relay Users*, *supra* note 28 (estimating that around 20% of the Tor Network's daily users are based in the United States).

114. Targeting on the dark web is blind; investigators do not know where the target is located and thus cannot control the route network investigative techniques take to get there. *See* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1072-73 (2001).

115. *See* Letter from Peter J. Kadzik, Assistant Att'y Gen., U.S. Dep't of Justice, to Sen. Charles E. Grassley, Chairman, Senate Judiciary Comm. 2 (July 14, 2015) (on file with author).

116. Ghappour, *supra* note 26.

117. *See supra* note 48.

relations risks that may be incurred call into question the wisdom of allowing rank-and-file officials to drive decisionmaking as to what crimes should trigger the use of hacking techniques, what hacking techniques should be used, and whose property interests may be targeted.

II. Law Enforcement out of Bounds

A. Conventional Methods Are in Harmony with International Law

International law delimits one state's power over another state's territorial sovereignty[118] by restricting states' exercise of prescriptive, adjudicative, and enforcement jurisdiction.[119] In the context of criminal law, the United States exercises *prescriptive* jurisdiction when Congress enacts statutes that criminalize conduct and *enforcement* jurisdiction when its law enforcement agencies investigate, apprehend, or prosecute a wrongdoer.[120]

Prescriptive jurisdiction and enforcement jurisdiction "are not geographically coextensive."[121] International law is most permissive with respect to

118. Territorial sovereignty can be defined as the principle that each state is coequal and has the final authority within its territorial limits. *See* Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 IND. J. GLOBAL LEGAL STUD. 475, 476 & n.5 (1998) (citing Stephen D. Krasner, *Sovereignty: An Institutional Perspective*, 21 COMP. POL. STUD. 66, 86 (1988) ("The assertion of final authority within a given territory is the core element in any definition of sovereignty."); and Janice E. Thomson, *Sovereignty in Historical Perspective: The Evolution of State Control over Extraterritorial Violence*, *in* THE ELUSIVE STATE: INTERNATIONAL AND COMPARATIVE PERSPECTIVES 227, 227 (James A. Caporaso ed., 1989) ("Despite their debate over whether the state is a withering colossus or a highly adaptive entity . . . , international relations theorists agree on an even more fundamental point. Both liberal interdependence and realist theories rest on the assumption that the state controls at least the principal means of coercion.")); *see also* Island of Palmas (U.S. v. Neth.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) ("Sovereignty in the relations between States signifies . . . the right to exercise [on its territory], to the exclusion of any other States, the functions of a State.").

119. Broadly, "jurisdiction" can be defined as a state's "right under international law to regulate matters not exclusively of domestic concern." *See* F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECUEIL DES COURS 9, 9 (1964). "Prescriptive jurisdiction" refers to a state's ability "to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things." RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 401(a) (AM. LAW INST. 1987). "Adjudicative jurisdiction" is defined as a state's ability "to subject persons or things to the process of its courts or administrative tribunals." *Id.* § 401(b). "Enforcement jurisdiction" refers to a state's ability to "compel compliance . . . with its laws." *Id.* § 401(c).

120. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(1).

121. FTC v. Compagnie de Saint-Gobain-Pont-a-Mousson, 636 F.2d 1300, 1316 (D.C. Cir. 1980).

prescriptive jurisdiction. It permits a state to criminalize conduct that occurs beyond its borders so long as the prescribed conduct has territorial effects.[122] But "[a] state having jurisdiction to prescribe a rule of law does not necessarily have jurisdiction to enforce it in all cases."[123] "[U]nlike a state's prescriptive jurisdiction, which is not strictly limited by territorial boundaries, enforcement jurisdiction by and large continues to be strictly territorial."[124] Indeed, there is unanimous consensus among states that "no state may engage in an act of coercion in the territory of another state without the latter's consent."[125]

Thus, while Congress may criminalize conduct that occurs wholly overseas so long as it has domestic "effects,"[126] international law forbids U.S. investigators from directly exercising law enforcement functions in other countries without first obtaining consent.[127] "[A] state cannot investigate a

122. *See* United States v. Aluminum Co. of Am., 148 F.2d 416, 443 (2d Cir. 1945) ("[A]ny state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends . . . ."). The application of federal statutes to overseas acts is permissible under international law only if the criminalized conduct has or is intended to have harmful effects on U.S. territory, nationals, or security interests; is a universally condemned offense; or was committed by a U.S. national. *See Draft Convention on Jurisdiction with Respect to Crime*, 29 AM. J. INT'L L. 435, 439-42 (Supp. 1935); *see also* INT'L BAR ASS'N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11-16 (2009), http://www.ibanet.org/Document/Default.aspx?DocumentUid=ECF39839-A217-4B3D-8106-DAB716B34F1E (noting that "states have long recognized the right of a state to exercise jurisdiction over persons or events located outside its territory in certain circumstances, based on the effects doctrine, the nationality or personality principle, the protective principle[,] or the universality principle" and providing an overview of each basis of jurisdiction).

123. *Saint-Gobain*, 636 F.2d at 1316 (alteration in original) (quoting RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 7(1) (AM. LAW INST. 1965)).

124. *Id.*; *see also* Hannah L. Buxbaum, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict*, 57 AM. J. COMP. L. 631, 664 (2009).

125. Buxbaum, *supra* note 124, at 664; *see also* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2); JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 478-79 (8th ed. 2012). The principle of nonintervention prohibits all acts that are intended "to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind." G.A. Res. 2625 (XXV), annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations (Oct. 24, 1970).

126. As a matter of domestic law, Congress may extend the reach of the criminal law extraterritorially, subject to constitutional limits. Knox, *supra* note 37, at 351 n.1 ("Congress could decide to exceed [international law limits] if it chose to place the United States in violation of international law."); *see* Brilmayer & Norchi, *supra* note 37, at 1223 (arguing for jurisdictional limits on legislative authority that sound in constitutional due process).

127. *See, e.g.*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly

footnote continued on next page

crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission."[128] Nonetheless, using conventional mechanisms, U.S. criminal investigators collect digital evidence located anywhere in the world while limiting the exercise of enforcement mechanisms to the territorial United States.[129]

The evidence collection methods authorized under the pre-amendment version of the Federal Rules of Criminal Procedure are in harmony with international law's restrictions on enforcement jurisdiction. Despite their global reach, the rules of criminal procedure may only be enforced with respect to persons and property that touch the United States.[130]

In this context, digital evidence collection can be divided into direct and indirect collection mechanisms. Direct collection typically involves coerced entry[131] into a place by government actors for the purpose of acquiring evidence of a crime, and it typically requires a search warrant.[132] Indirect collection, by contrast, involves service of a subpoena or court order that

authorized officials of that state."); CRYER ET AL., *supra* note 38, § 3.2.3, at 44 (using the term "executive jurisdiction" to discuss enforcement jurisdiction and defining it as "the right to effect legal process coercively, such as to arrest someone, or undertake searches and seizures"); *see also* Alvarez-Machain v. United States, 331 F.3d 604, 625 (9th Cir. 2003) (en banc) ("Extraterritorial *application* [of a criminal statute] . . . does not automatically give rise to extraterritorial *enforcement* authority."), *rev'd on other grounds sub nom.* Sosa v. Alvarez-Machain, 542 U.S. 692 (2004).

128. INT'L BAR ASS'N, *supra* note 122, at 10.

129. *See infra* notes 130-53 and accompanying text.

130. *Cf.* 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 432 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) ("[T]he interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."); Maziar Jamnejad & Michael Wood, *The Principle of Non-Intervention*, 22 LEIDEN J. INT'L L. 345, 372 (2009) ("The exercise of enforcement jurisdiction in the territory of another state, without its consent, breaches the non-intervention principle. . . . [E]xtraterritorial enforcement measures will nearly always be considered illegal [under customary international law].").

131. Direct collection includes forcibly entering a space where the targeted device is located and subsequently bypassing security restrictions on that device. However, entry or access need not cause physical damage to be "coerced." *See, e.g.*, Calabretta v. Floyd, 189 F.3d 808, 813 (9th Cir. 1999).

132. This type of government conduct typically falls under the Warrant Clause of the Fourth Amendment, which requires investigators to first obtain a search warrant before performing the collection activity. *See* U.S. CONST. amend. IV. A search warrant constitutes the judicial authorization, made upon a finding of probable cause, of an activity that is uniquely assigned to law enforcement—intruding upon an individual's reasonable expectation of privacy to conduct a search and seizure. A search warrant is self-executing; it authorizes an investigator to directly coerce entry or access to, and extraction of digital evidence from, a computer or electronic media. *See, e.g.*, Marshall v. Barlow's, Inc., 436 U.S. 307, 316 (1978) (explaining that searches may be "executed without delay and without prior notice, thereby preserving the element of surprise"); *see also Search Warrant*, BLACK'S LAW DICTIONARY (10th ed. 2014).

imposes an affirmative duty on its recipient to either produce evidence under that recipient's control or face sanctions for noncompliance.[133] In the digital context, a physical seizure of a computer is a direct collection, as is the use of network investigative techniques. The subpoena power, on the other hand, is an indirect collection mechanism, as is the use of compelled technical assistance to conduct a wiretap.

Direct collection of foreign-located evidence using conventional methods is an obvious exercise of enforcement jurisdiction.[134] Criminal procedure requires direct collection of digital evidence to be conducted pursuant to a search warrant, which authorizes investigators to exercise coercive "search and seizure" powers directed toward a particular place to be searched or thing to be seized.[135] Investigators executing a search warrant may use coercive force and may even damage the targeted items or premises when necessary to effectuate a particular search or seizure.[136]

Search warrant authority (and direct collection methods exercised under search warrant authority) does not generally extend beyond the territorial United States.[137] Federal Rule of Criminal Procedure 41 generally restricts a

133. *See, e.g.*, *In re* Grand Jury Proceedings the Bank of N.S., 740 F.2d 817, 829 (11th Cir. 1984) (holding that a Canadian bank operating in the United States was obliged to produce documents located in the Cayman Islands in response to a grand jury subpoena); *see also In re* Grand Jury Subpoena Directed to Marc Rich & Co., 707 F.2d 663, 667 (2d Cir. 1983) ("The test for the production of documents is control, not location.").

134. As Justice Joseph Story explained in 1841, territorial sovereignty implies that "no state or nation can, by its laws, *directly* affect, or bind property out of its own territory, or bind persons not resident therein." JOSEPH STORY, COMMENTARIES ON THE CONFLICT OF LAWS, FOREIGN AND DOMESTIC, IN REGARD TO CONTRACTS, RIGHTS, AND REMEDIES, AND ESPECIALLY IN REGARD TO MARRIAGES, DIVORCES, WILLS, SUCCESSIONS, AND JUDGMENTS § 20 (Boston, Charles C. Little & James Brown 2d ed. 1841) (emphasis added); *see also* Goldsmith, *supra* note 118, at 480.

135. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that officers must generally secure a search warrant before conducting a search of data stored on a smartphone confiscated incident to a lawful arrest); *Calabretta*, 189 F.3d at 813 ("The principle that government officials cannot coerce entry into people's houses without a search warrant or applicability of an established exception to the requirement of a search warrant is so well established that any reasonable officer would know it.").

136. *See, e.g.*, *In re* Subpoena Duces Tecum, 228 F.3d 341, 348 (4th Cir. 2000) ("To preserve advantages of speed and surprise, [a warrant] is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion.").

137. In 1990, the Supreme Court, ruling that foreign-located nonresident aliens are not entitled to Fourth Amendment protection, strongly suggested that the Warrant Clause has no extraterritorial application. United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990); *see also In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 169 (2d Cir. 2008) ("[I]n *Verdugo-Urquidez*, seven justices of the Supreme Court endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches."); United States v. Barona, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) ("[F]oreign searches have neither been historically subject to the warrant procedure, nor could they be as a practical matter."); United States v. Bin Laden, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000)
footnote continued on next page

court's authority to issue warrants to the district of the magistrate making the decision.[138] Exceptions are generally limited to instances in which the search warrant relates to American diplomatic or consular missions in foreign states.[139] Indeed, any collection of evidence that requires an assertion of extraterritorial enforcement jurisdiction triggers the formal and informal cooperation protocols discussed in Part I.B above.

Indirect collection of foreign-located evidence, by contrast, does not require the exercise of enforcement jurisdiction overseas. Instead, compelled disclosure orders impose an affirmative duty on third parties to disclose evidence in their possession or control in response to a specific request.[140] A person or entity that fails to produce evidence in its control may face domestic sanctions for noncompliance.[141] Critically, the steps of the collection act—accessing and extracting foreign-located data—are performed by third parties, not state actors.[142]

In practice, courts regularly issue and uphold orders that compel disclosure of foreign-located evidence from third parties, so long as the third party falls under the court's personal jurisdiction and has control over the evidence.[143]

("[T]here is presently no statutory basis for the issuance of a warrant to conduct searches abroad."), *aff'd in part, vacated in part, and remanded*, 552 F.3d 157 (2d Cir. 2008).

138. *See* FED. R. CRIM. P. 41(b)(1).

139. *Id.* 41(b)(5) (permitting out-of-district warrants to conduct searches in U.S. territories overseas and on the premises of diplomatic or consular missions in foreign states); *see id.* advisory committee's note to 2008 amendment ("The rule is intended to authorize a magistrate judge to issue a search warrant in any of the locations for which 18 U.S.C. § 7(9) provides jurisdiction."); *see also* 18 U.S.C. § 7 (2015) (defining the special maritime and territorial jurisdiction of the United States); *cf.* Note, *Criminal Jurisdiction over Civilians Accompanying American Armed Forces Overseas*, 71 HARV. L. REV. 712, 712 n.5 (1958) (noting that at the time, there were no treaties providing consent other than Status of Forces Agreements and that the "United States can exercise jurisdiction over its civilians within a foreign territory only with the sovereign's prior consent"). For an excellent treatment of the extraterritorial aspects of U.S. criminal enforcement jurisdiction under Status of Forces Agreements, see JOSEPH M. SNEE & A. KENNETH PYE, STATUS OF FORCES AGREEMENTS AND CRIMINAL JURISDICTION 92-109 (1957).

140. *See* FED. R. CRIM. P. 17(c)(1); *see also Subpoena*, BLACK'S LAW DICTIONARY (10th ed. 2014) (defining a "subpoena" as a "writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply," and defining a "subpoena duces tecum" as an order requiring a person "to appear in court and to bring specified documents, records, or things").

141. *See supra* note 133.

142. *See, e.g.*, *In re* Grand Jury Proceedings the Bank of N.S., 740 F.2d 817, 832 (11th Cir. 1984).

143. *See, e.g.*, *id.* at 826-28 (ordering production of evidence despite Cayman Island bank secrecy laws); *In re* Grand Jury Subpoena Directed to Marc Rich & Co., 707 F.2d 663, 665, 670 (2d Cir. 1983) (affirming an order to produce evidence despite a claim that it would violate Swiss law); United States v. Vetco Inc., 691 F.2d 1281, 1286-87 (9th Cir. 1981) (ordering production despite possible criminal penalties under Swiss law); *In re* Grand Jury Subpoena Served upon Simon Horowitz, 482 F.2d 72, 79-80 (2d Cir. 1973)

footnote continued on next page

Courts applying this principle have observed that "the operation of foreign law 'do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law].'"[144]

In the digital context, the steps of indirect collection are much the same as in the physical world.[145] For example, law enforcement may apply for court orders requiring U.S.-based providers to disclose digital evidence in their possession.[146] The recipient of such orders may comply by providing the requested evidence. If she does not comply and cannot show good cause, she may face judicial enforcement in the form of civil contempt sanctions.[147]

(Friendly, J.) (upholding in part a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client); Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *11-12 (C.D. Cal. May 29, 2007) (ordering a party to produce digital evidence stored on servers in the Netherlands, despite the fact that doing so would violate Dutch privacy law); United States v. Chase Manhattan Bank, 584 F. Supp. 1080, 1086-87 (S.D.N.Y. 1984) (requiring production despite a Hong Kong judge's bank secrecy order).

144. Linde v. Arab Bank, 706 F.3d 92, 109 (2d Cir. 2013) (alterations in original) (quoting Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court, 482 U.S. 522, 544 n.29 (1987)).

145. *See* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 134 (n.d.), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter CCIPS GUIDELINES] ("[I]nvestigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant."). The operational trajectory is the same as the subpoena process. First, the court order is obtained. Second, the ISP is served with the order. Third, the third-party service provider gives law enforcement responsive evidence. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1222-24 (2004) (citing 18 U.S.C. §§ 2702-2703, 2711) (describing the steps of using the Stored Communications Act (SCA) to collect digital evidence).

146. Depending on the type of information an order seeks, law enforcement is required to show varying levels of suspicion. *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620 tbl.2, 621 (2003) (describing "the continuum of court orders and legal processes" that the SCA uses to govern law enforcement collection of digital evidence); *see also* CCIPS GUIDELINES, *supra* note 145, at 127 ("Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some).").

147. Recently, the Second Circuit held that, as a matter of statutory interpretation, compelled disclosure of digital evidence under the SCA, a thirty-year-old statute, does not apply to customer data stored outside the United States. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 201 (2d Cir. 2016), *reh'g en banc denied*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017). However, such extraterritoriality would be consistent with the U.S. Constitution and international law's bounds on enforcement jurisdiction, as would use of a grand

footnote continued on next page

Critical to criminal procedure's compliance with international norms, the United States is not authorized to "enforce its laws against an individual content provider from another country unless the content provider has a local presence."[148] Indeed, congressionally enacted enforcement mechanisms for indirect collection are territorial; the courts may order forfeiture only of domestic property.[149]

Collection of foreign-located data using compulsory process complies with international law's restrictions on enforcement jurisdiction so long as the enforcement mechanisms are limited to persons and property within the United States.[150] By leveraging the threat of territorial enforcement (for instance, through an order authorizing seizure of property upon a finding of contempt), law enforcement is able to require companies to produce foreign-located evidence.[151] The United States takes no direct extraterritorial acts when it compels disclosures and receives information despite the fact that the motivating factor for the third party is the threat of U.S. (territorial) enforcement.[152] All acts taken on foreign soil—including retrieval of foreign-stored information and its transport to the United States—are performed by a third party.[153]

---

jury subpoena to seek the same customer data stored outside the United States. *See infra* notes 150-53 and accompanying text.

148. Goldsmith, *supra* note 118, at 485.

149. When a court enters such orders, it exercises territorial enforcement jurisdiction. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 431 cmt. b (AM. LAW INST. 1987). Law enforcement authorities, too, exercise enforcement jurisdiction in executing such orders. *Id.* cmt. c.

150. *Cf. In re* Petition of Boehringer Ingelheim Pharm., Inc., 745 F.3d 216, 218 (7th Cir. 2014) (Posner, J.) (noting that foreign nationals outside U.S. territory are beyond the court's subpoena power).

151. *Id.* at 216-18.

152. In a case involving a U.S. discovery order relating to French witnesses and documents, the court found that the order did not intrude on French sovereignty or judicial custom. Adidas (Can.) Ltd. v. S.S. Seatrain Bennington, Nos. 80 Civ. 1911 (PNL), 82 Civ. 0375 (PNL), 1984 WL 423, at *2 (S.D.N.Y. May 30, 1984). The court concluded:

> No adverse party will enter on French soil to gather evidence (or otherwise). No oath need be administered on French soil or by a French judicial authority.
>
> What is required . . . on French soil is certain acts preparatory to the giving of evidence. [The company] must select appropriate employees to give depositions in the forum state: likewise it must select the relevant documents which it will reveal to its adversaries in the forum state. These acts do not call for French judicial participation. . . . In no way do those acts affront or intrude on French sovereignty.

Id.; *see also In re* Anschuetz & Co., 754 F.2d 602, 611 (5th Cir. 1985) (concluding that a district court's ordering of depositions to be conducted on German soil was not a violation of international law).

153. *Adidas (Can.)*, 1984 WL 423, at *2; *accord In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 476 (S.D.N.Y. 2014) (holding that an order for compelled process "places obligations only on the

footnote continued on next page

B. Failure of the Existing Rules

The harmony[154] between conventional evidence-gathering methods and international law's restrictions on extraterritorial enforcement jurisdiction begins to unravel with the practice of network investigative techniques on the dark web. The amendment to Rule 41 governing search warrant venue requirements did little more than remove a procedural hurdle in the way of courts' ability to issue warrants for territorial law enforcement searches and seizures.[155] In applying the legal process for search warrants to network investigative techniques, law enforcement and courts assume that anonymized targets are territorially located during all stages of implementation and enforcement.[156] After all, courts lack constitutional and statutory authority to issue extraterritorial warrants, and any such warrant would have no force in a foreign state without an agreement to the contrary.[157]

Application of the existing rules to anonymized targets results in a bizarre structural arrangement: the courts have no authority over the extraterritorial aspect of network investigative techniques, yet the issuance of search warrants is a condition precedent to their execution. Network investigative techniques that wind up targeting computers in the territorial United States are authorized by warrant, while those that land overseas draw authority directly

service provider to act"), *rev'd, vacated, and remanded*, 829 F.3d 197 (2d Cir. 2016), *reh'g en banc denied*, No. 14-2985, 2017 WL 362765 (2d Cir. Jan. 24, 2017).

154. As summarized by James Crawford, U.S. courts "have taken the view that whenever activity abroad has consequences or effects within the US which are contrary to local legislation then the American courts may make orders requiring the . . . production of documents." CRAWFORD, *supra* note 125, at 479-80 ("Such orders may be enforced by action within the US against individuals or property present within [U.S.] territorial jurisdiction . . . .").

155. *See* Memorandum from David Bitkower, Deputy Assistant Att'y Gen., U.S. Dep't of Justice, to Judge Reena Raggi, Chair, Advisory Comm. on Rules of Criminal Procedure 2 (Oct. 20, 2014), *in* ADVISORY COMM. ON CRIMINAL RULES, *supra* note 32, at 133, 134 ("What our proposal would accomplish is untying the hands of law enforcement when it is not yet known whether the Fourth Amendment requires a warrant because it is unknown whether the media is in the United States—and it accomplishes that by ensuring that a judge is available to hear the warrant application.").

156. For example, one application requested and was granted a warrant to infect every computer that associated with a server located in Virginia. *See* United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *4 (W.D. Wash. Jan. 28, 2016). The location listed on the warrant application was Virginia, even though it authorized over 8000 malware infections of computers located in 120 countries. Cox, *FBI Hack*, *supra* note 27 ("As far as is publicly known, these mass hacking techniques have been limited to child pornography investigations. But with the changes to Rule 41, there is a chance US authorities will expand their use to other crimes too.").

157. *See* United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 318 (1936).

from the executive's plenary powers to enforce the laws of the United States[158] and from statutes authorizing the DOJ and FBI to investigate individuals for violations of U.S. laws.[159]

As for intra-agency checks and balances, the DOJ's existing protocols on cross-border investigations cannot be applied before the deployment of network investigative techniques on the dark web because investigators are unable to discern a target's location until after it has been hacked. For example, investigators are required to "use reasonable efforts to ascertain whether any pertinent computer system, data, witness, or subject is located in a foreign jurisdiction" and "follow the policies and procedures set out by their agencies for international investigations" to gather evidence located overseas.[160] These procedures typically include consultation with the DOJ's Computer Crime and Intellectual Property Section (CCIPS)—the DOJ's technology section—or the

158. This would require finding that pursuant to the constitutional command to "take Care that the Laws be faithfully executed," U.S. CONST. art. II, § 3, "the President has the power to authorize agents of the executive branch to engage in law enforcement activities in addition to those provided by statute," Auth. of the FBI to Override Int'l Law in Extraterritorial Law Enf't Activities, 13 Op. O.L.C. 163, 176 (1989). Whether the mechanics of such authority violate the separation of powers is beyond the scope of this Article. For the purposes of this Article, I concede the claim that the Take Care Clause, in conjunction with the broad authorizing statutes carrying into execution core executive powers, gives the President raw authority to make these decisions and to delegate them to nonappointed members of the DOJ. *See Auth. of the FBI*, 13 Op. O.L.C. at 176. The 1989 Office of Legal Counsel opinion effectively overruled an opinion from 1980, which concluded that the FBI may not conduct extraterritorial apprehensions in violation of international law. *See* Extraterritorial Apprehension by the FBI, 4B Op. O.L.C. 543, 549 (1980).

159. *See* 18 U.S.C. § 3052 (2015); 28 U.S.C. § 533(1) (2015). The question whether by enacting these statutes Congress delegated authority to the DOJ and the FBI to violate international law has not been addressed by the courts and is beyond the scope of this Article. Under *Chevron*, "[i]f . . . the court determines Congress has not directly addressed the precise question at issue, . . . the question for the court is whether the agency's answer [here, that it has authority to violate international law] is based on a permissible construction of the statute." Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 843 (1984). Scholars disagree regarding the extent of the deference owed the executive branch in the context of ambiguous statutory authority. *Compare* Eric A. Posner & Cass R. Sunstein, Chevron*izing Foreign Relations Law*, 116 YALE L.J. 1170, 1220 (2007) (arguing that with respect to the Authorization for Use of Military Force passed by Congress in September 2001, "the President should be taken to have the authority to interpret ambiguities as he chooses"), *with* Derek Jinks & Neal Kumar Katyal, *Disregarding Foreign Relations Law*, 116 YALE L.J. 1230, 1236 (2007) (rejecting enhanced judicial deference in foreign affairs in the "executive constraining zone").

160. ONLINE INVESTIGATIONS WORKING GRP., U.S. DEP'T OF JUSTICE, ONLINE INVESTIGATIVE PRINCIPLES FOR FEDERAL LAW ENFORCEMENT AGENTS 62 (1999) (bolding omitted). The guidelines note "the difficulties inherent in ascertaining physical location in an online environment" and instruct law enforcement agents to "seek guidance if they suspect a transborder issue may arise." *Id.* at 63.

OIA[161] and often require written approval before using unilateral compulsory measures for information located overseas.[162] However, if investigators lack knowledge of a target's location, they cannot effectively use these procedures.

In the regulatory vacuum that results, rank-and-file officers have discretion that may shape U.S. policy regarding which crimes trigger the use of cross-border network investigative techniques, the breadth of hacking techniques that are used to effectuate remote searches, and whose property may be targeted. Moreover, although the ex ante warrant process regulates some aspects of network investigative techniques, it does so without regard to national security or international norms. A warrant may impose constitutional limitations that check the intensity and breadth of hacking techniques. But cross-border cyberoperations will still be unilateral, invasive, and conducted without coordination with the agencies that lead U.S. foreign relations and national security policy.

C. The Foreign Relations Risk of Hacking the Dark Web

Law enforcement's use of network investigative techniques on the dark web is in obvious tension with international norms. It is not clear whether (and to what extent) a particular network investigate technique runs afoul of international law or how targeted states may respond. This uncertainty gives rise to five categories of risk: (1) the risk of attribution, (2) the risk of vulnerability disclosure, (3) diplomatic risks associated with unauthorized cross-border operations, (4) the risk of foreign prosecution targeting U.S. law enforcement members, and (5) the risk of countermeasures the injured state may be entitled to take.

1. The risk of attribution

The risk of attribution faced by investigators for cross-border network investigative techniques is heightened due to the FBI's operational protocols and the public nature of the criminal justice system. For example, in a recent case the government was ordered to disclose information about thousands of

161. *See* CCIPS GUIDELINES, *supra* note 145, at 57-58; OFFICES OF THE U.S. ATT'YS, U.S. ATTORNEYS' MANUAL § 9-13.500 (1997) (requiring prosecutors to seek approval from the OIA when seeking any assistance abroad or taking "any act outside the United States relating to a criminal investigation or prosecution").

162. *See* OFFICES OF THE U.S. ATT'YS, *supra* note 161, § 9-13.525 ("[A]ll Federal prosecutors must obtain written approval through the Office of International Affairs (OIA) before issuing any subpoenas to persons or entities in the United States for records located abroad."). The U.S. Attorneys' Manual and departmental policy guidance instruct prosecutors on when and how to make a request for approval and assistance from the OIA.

computers located in over a hundred foreign countries.[163] This requirement conflicted with defense and intelligence policy mandating secrecy for cross-border cyberoperations.

This dynamic introduces an asymmetry against the United States: U.S. attribution of harmful attacks to states is based on circumstantial evidence that is typically not definitive (and thus of questionable legitimacy, particularly when faced with denial by the accused country), whereas attribution to the United States of cross-border network investigative techniques is much more defensible because it is more likely to be based on official documents.[164]

The attribution issue was highlighted by the November 2014 breach at Sony Pictures Entertainment by a group calling themselves the "Guardians of Peace."[165] In December 2014, the FBI attributed the hack to the North Korean government.[166] In its attribution, the FBI cited malware linked "to other malware that the FBI knows North Korean actors previously developed" in a 2013 attack of South Korean banks and media outlets.[167] Additionally, the agency noted "significant overlap between the infrastructure used in this attack and other malicious cyber activity the U.S. government has previously linked directly to North Korea."[168] However, experts critical of this attribution correctly note that the evidence is not definitive.[169] Further fueling speculation, officials have not revealed specifics as to how they determined North Korea was responsible, likely due to the involvement of the National Security Agency (NSA) and consequent classification of the information.[170]

---

163. *See* Transcript of Evidentiary Hearing at 39, United States v. Tippens, No. CR16-5110RJB (W.D. Wash. Nov. 1, 2016); Cox, *FBI Hack*, *supra* note 27.

164. Without evidence of attribution satisfying the reasonable doubt standard, for example, the United States would not be able to prosecute a state actor alleged to have violated U.S. law by hacking into a computer in the United States.

165. The FBI, in its investigation, noted that the breach "consisted of the deployment of destructive malware and the theft of proprietary information as well as employees' personally identifiable information and confidential communications. The attacks also rendered thousands of [Sony]'s computers inoperable, forced [Sony] to take its entire computer network offline, and significantly disrupted the company's business operations." Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

166. *Id.*

167. *Id.*

168. *Id.*

169. *See, e.g.*, Bruce Schneier, *We Still Don't Know Who Hacked Sony*, ATLANTIC (Jan. 5, 2015), http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198; *see also* David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES (Jan. 2, 2015), http://nyti.ms/1ygfN0V.

170. *See* Sanger & Schmidt, *supra* note 169.

2. The risk of vulnerability disclosure

The use of network investigative techniques also raises national security risks related to the use and disclosure of software vulnerabilities. A "zero-day" vulnerability is a software bug for which no patch exists.[171] Malicious code exploiting zero-day vulnerabilities can propagate from one computer to the next with impunity.[172] Zero-day exploits are valuable because owning a zero-day exploit, in principle, provides the capability to penetrate any device in the world running the affected software until the developer rolls out a software update that patches the security flaw.[173]

Intelligence agencies, whose mandate includes protecting the nation's cyberinfrastructure from attack, generally have a greater interest in vulnerability disclosure.[174] To be sure, intelligence agencies also have an interest in exploiting vulnerabilities to accomplish intelligence-gathering objectives through cross-border hacking—which they no doubt value more than law enforcement interests.[175] However, the intelligence community has

171. Andrea Peterson, *Why Everyone Is Left Less Secure When the NSA Doesn't Help Fix Security Flaws*, WASH. POST (Oct. 4, 2013), http://wpo.st/sGT42. The name reflects the number of days such a bug has been known to the software developer. *See* Kim Zetter, *Turns Out the US Launched Its Zero Day Policy in Feb 2010*, WIRED (June 26, 2015, 9:48 AM), https://www.wired.com/2015/06/turns-us-launched-zero-day-policy-feb-2010. *See generally* Jason Healy, *The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers*, J. INT'L AFF. (Nov. 1, 2016), https://jia.sipa.columbia.edu/online-articles/healey_vulnerability_equities_process (criticizing the FBI's decision to contract with an undisclosed firm to unlock the iPhone used by San Bernardino shooter Syed Farook).

172. *See* Ryan Gallagher, *Cyberwar's Gray Market: Should the Secretive Hacker Zero-Day Exploit Market Be Regulated?*, SLATE (Jan. 16, 2013, 9:00 AM), http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html; Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, WIRED (Apr. 17, 2015, 6:25 AM), https://www.wired.com/2015/04/therealdeal-zero-day-exploits; Andrea Peterson, *A Company That Sells Hacking Tools to Governments Just Got Hacked*, WASH. POST (July 6, 2015), http://wpo.st/cQT42.

173. Tom Gjelten, *In Cyberwar, Software Flaws Are a Hot Commodity*, NPR (Feb. 12, 2013, 3:25 AM ET), https://n.pr/WVasXe; *see* Vlad Tsyrklevich, *Hacking Team: A Zero-Day Market Case Study*, TSYRKLEVICH.NET (July 22, 2015), https://tsyrklevich.net/2015/07/22/hacking-team-0day-market.

174. *See* Malena Carollo, *Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research*, CHRISTIAN SCI. MONITOR (Sept. 29, 2015), http://fw.to/sI9NwEJ; *see also* Jack Detsch, *Influencers Oppose Expanding Federal Hacking Authorities*, CHRISTIAN SCI. MONITOR (May 9, 2016), http://passcode.csmonitor.com/influencers-rule41 (describing how, in a survey of experts from across the government, the technology and security industry, and the privacy advocacy community, "[n]early two-thirds of Passcode's Influencers said [U.S.] judges should not be able to issue search warrants for computers located outside their jurisdictions").

175. *See* David E. Sanger, *Obama Lets N.S.A. Exploit Some Internet Flaws, Officials Say*, N.Y. TIMES (Apr. 12, 2014), http://nyti.ms/1gmYqOm.

more sophisticated hacking capabilities than law enforcement and can therefore be much more selective about the vulnerabilities it withholds for intelligence gathering.[176] By contrast, law enforcement agencies have an interest in keeping a larger pool of vulnerabilities unpatched in order to use hacking techniques in pursuit of criminal suspects. The conflict has played out before the White House Vulnerabilities Equities Process—an administrative proceeding before an Equities Review Board chaired by the National Security Council—which the FBI has been criticized for bypassing entirely.[177]

The government's use of malware also risks exposing these vulnerabilities to criminals or malicious state actors. When a criminal or foreign agent accesses a computer hacked by the United States, he may be able to reverse-engineer the attack in order to use it to attack cyberinfrastructure in the United States.[178] In May 2016, software maker Mozilla filed a motion asking the FBI to disclose a potential vulnerability in the Firefox browser that the FBI allegedly used to hack visitors of a child pornography site,[179] "trigger[ing] a fierce debate around the responsibility of governments to disclosure [sic] vulnerabilities used in investigations to affected companies."[180] The software maker underscored the cybersecurity implications of the vulnerability, arguing in its motion to intervene that "the security of millions of individuals using Mozilla's Firefox Internet browser could be put at risk by a premature disclosure of this vulnerability."[181]

In a recent case the government was ordered to disclose its hacking tools' source code to the defense, but its compliance with the order was blocked by the FBI, which asserted that disclosure of the vulnerability information would

176. *See id.*

177. *See* Healy, *supra* note 171.

178. Amy Zegart, *Vladimir Putin Is Trying to Hack the Election: What Should US Do?*, CNN (Oct. 24, 2016, 12:18 PM ET), http://cnn.it/2exPWwu ("Many cyber weapons have a 'use it and lose it' quality. Once they are in the wild, they can be reverse engineered and possibly used against us.").

179. Mozilla's Motion to Intervene or Appear as Amicus Curiae in Relation to Government's Motion for Reconsideration of Court's Order on the Third Motion to Compel at 1-2, United States v. Michaud, No. 15-CR-05351-RJB (W.D. Wash. May 11, 2016) [hereinafter Mozilla's Motion to Intervene]; Joseph Cox, *Mozilla Urges FBI to Disclose Potential Firefox Security Vulnerability*, MOTHERBOARD (May 12, 2016, 12:26 AM), http://motherboard.vice.com/read/mozilla-urges-fbi-to-disclose-firefox-security-vulnerability.

180. Cox, *supra* note 179.

181. Mozilla's Motion to Intervene, *supra* note 179, at 1-2 ("To protect the safety of Firefox users, and the integrity of the systems and networks that rely on Firefox, Mozilla requests that the Court order that the Government disclose the exploit to Mozilla at least 14 days before any disclosure to the Defendant, so Mozilla can analyze the vulnerability, create a fix, and update its products before the vulnerability can be used to compromise the security of its users' systems by nefarious actors.").

have subjected the United States to national security risk.[182] At least one court has found that the refusal to disclose an exploit to the defense requires the suppression of any evidence obtained as a result of the technique.[183]

3. The risk to diplomatic legitimacy

The United States has an interest in taking a leadership role in norm development in cyberspace.[184] Harmonization between states is facilitated through diplomacy.[185] Hard diplomacy is the negotiation of treaties and other formal agreements.[186] It functions through formal, traditional channels of negotiation between the officials of two or more states or through an international organization like the United Nations. Soft diplomacy relies on indirect influence through interactions with civilians and government actors.[187] According to Joseph Nye, a state's soft power turns on "its culture (in places where it is attractive to others), its political values (when it lives up to

182. *See* Charlie Osborne, *FBI Refuses to Release Tor Exploit Details, Evidence Thrown out of Court*, ZDNET (May 26, 2016, 9:55 GMT), http://zd.net/1sc15XX ("There are 1,200 cases pending against alleged visitors to the website and the formal refusal of evidence gained by tracking these visitors could destroy the FBI's hopes of winning these cases. Without being able to submit evidence that each defendant viewed or downloaded child abuse images, many—if not all—of these cases are at risk of collapse.").

183. *See* Order Denying Dismissal & Excluding Evidence at 1, *Michaud*, No. 3:15-CR-05351-RJB (W.D. Wash. May 25, 2016); *see also* Osborne, *supra* note 182.

184. The Department of Defense (DoD) Strategy for Operating in Cyberspace states:

> Given the dynamism of cyberspace, nations must work together to defend their common interests and promote security. DoD's relationship with U.S. allies and international partners provides a strong foundation upon which to further U.S. international cyberspace cooperation. Continued international engagement, collective self-defense, and the establishment of international cyberspace norms will also serve to strengthen cyberspace for the benefit of all.

U.S. Dep't of Def., Department of Defense Strategy for Operating in Cyberspace 2 (2011), http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

185. *See* Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 146 (2000) ("When regulatory conflict and regulatory spillover occur with respect to 'real-space' transnational transactions, nations have responded with a variety of international harmonization strategies.").

186. *See id.* ("Sometimes harmonization takes the 'hard' form of treaties that either establish a uniform international standard, or an international anti-discrimination regime, or an international choice-of-law regime. Other times harmonization takes 'softer' forms like information sharing among enforcement agencies or informally agreed-upon regulatory targets.").

187. *Cf.* JOSEPH S. NYE, JR., THE FUTURE OF POWER 83 (2011) (noting the difficulties of incorporating soft power into a government's strategy because its instruments "are not fully under the control of governments," its outcomes are more in the control of the targeted state rather than the initiating state, and the results take a long time).

them at home and abroad), and its foreign policies (when others see them as legitimate and having moral authority)."[188]

Soft power is particularly useful in the cyberspace context because of attribution and enforcement difficulties. Therefore, the public scope and nature of cross-border cyberoperations may have heightened foreign policy consequences. This is where leading by example comes into play.[189] As Harold Koh has argued, the "process of visibly obeying international norms builds U.S. 'soft power,' enhances its moral authority, and strengthens U.S. capacity for global leadership."[190] It follows that the extent of the visible violations of our obligations to other nations—and our interpretation of those obligations—signals to the international community the United States' position as to what the existing norms permit and, more broadly, sends a significant message as to the United States' position on the rule of law.

The United States has taken the position that applying existing international norms to cyberspace is merely a matter of "applying old questions to the latest developments in technology."[191] Where there are many gaps in the application of existing law to new technologies,[192] the United States may have an interest in nudging norm development one way or another.[193] Yet the

188. *Id.* at 84.

189. *Cf.* United States v. Verdugo-Urquidez, 494 U.S. 259, 285 (1990) (Brennan, J., dissenting) ("Mutuality also serves to inculcate the values of law and order. By respecting the rights of foreign nationals, we encourage other nations to respect the rights of our citizens. Moreover, as our Nation becomes increasingly concerned about the domestic effects of international crime, we cannot forget that the behavior of our law enforcement agents abroad sends a powerful message about the rule of law to individuals everywhere.").

190. Harold Hongju Koh, *On American Exceptionalism*, 55 STAN. L. REV. 1479, 1480 (2003); *see id.* at 1480 n.2 ("Soft power rests on the ability to set the agenda in a way that shapes the preferences of others. . . . If I can get you to *want* to do what I want, then I do not have to force you to do what you do *not* want to do. If the United States represents values that others want to follow, it will cost us less to lead." (alteration in original) (quoting JOSEPH S. NYE, JR., THE PARADOX OF AMERICAN POWER: WHY THE WORLD'S ONLY SUPERPOWER CAN'T GO IT ALONE 9 (2002))).

191. *See* Harold Hongju Koh, International Law in Cyberspace, Remarks to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 8 (2012).

192. *See* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 335-52 (2015) (explaining the limitations of analogizing cyberspace to the high seas, outer space, or Antarctica for the purpose of applying existing legal norms).

193. *See* Henry Farrell, Council on Foreign Relations, Promoting Norms for Cyberspace 1 (2015), http://i.cfr.org/content/publications/attachments/Norms_CyberBrief.pdf; James Andrew Lewis, Ctr. for Strategic & Int'l Studies, Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms 1 (2014), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140225_Lewis_TransatlanticCybersecurity Norms.pdf ("Europe and the United States have a collective interest in the promotion of a stable international order based on the rule of law, open and equitable arrange-

footnote continued on next page

United States has not articulated—explicitly or implicitly through state practice—an intelligible principle that distinguishes one form of cross-border cyberexfiltration operation targeting persons or firms from the next. In this context, the use of network investigative techniques will no doubt draw criticism about the legitimacy of U.S. policy positions[194] and affect international efforts to regulate cyberoperations, all of which are still at an embryonic stage.[195]

By allowing rank-and-file officials to control how hacking warrants are executed, the existing legal process effectively allows the circumstances of the immediate investigation to dictate foreign policy interests in cultivating soft power. Decisionmaking at the rank-and-file level is driven by the immediate goals of a domestic criminal investigation as opposed to broader, more complex foreign policy goals. Primary decisionmaking lacks meaningful interagency coordination and is enforced by a judiciary whose umpiring capabilities are limited to preserving individual rights in the domestic sphere and who lack technological expertise to spot irregularities.[196]

---

ments for trade, and a commitment to democratic government and individual rights."); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-606, UNITED STATES FACES CHALLENGES IN ADDRESSING GLOBAL CYBERSECURITY AND GOVERNANCE 1, 30, 39 (2010) (finding that the "global aspects of cyberspace present key challenges to U.S. policy"—including challenges to the United States' ability to assert leadership in norm development, conduct interagency coordination, and pursue a consistent national strategy—and arguing that "the United States will be at a disadvantage in promoting its national interests in the realm of cyberspace" until those challenges are addressed).

194. *See* David E. Sanger, *Fine Line Seen in U.S. Spying on Companies*, N.Y. TIMES (May 20, 2014), http://nyti.ms/1j6nJVq ("China demands that the U.S. give it a clear explanation of its cybertheft, bugging and monitoring activities, and immediately stop such activity . . . ." (quoting statement from the Chinese Defense Ministry)); *see also* Jack Goldsmith, *The U.S. Corporate Theft Principle*, LAWFARE (May 21, 2014, 8:07 AM), http://www.lawfareblog.com/2014/05/the-u-s-corporate-theft-principle ("What the United States needs is an explanation convincing to audiences outside the United States about why its principle of corporate espionage is attractive beyond its furtherance of U.S. corporate and national security interests.").

195. For example, China suspended its participation in a U.S.-China working group on cybersecurity just after the May 2014 indictments. Ting Shi & Michael Riley, *China Halts Cybersecurity Cooperation After U.S. Spying Charges*, BLOOMBERG (May 20, 2014, 2:39 AM PDT), http://www.bloomberg.com/news/2014-05-20/china-suspends-cybersecurity-cooperation-with-u-s-after-charges.html; *see* Sanger, *supra* note 194.

196. According to one former magistrate, "judges who allow technological advances to pass them by aren't doing the public any favors by not staying current. Law enforcement has moved on, and it's tough to act as a check against overreach if you don't understand the subject matter." *See* Tim Cushing, *Judge John Facciola on Today's Law Enforcement: I'd Go Weeks Without Seeing a Warrant for Anything 'Tactile,'* TECHDIRT (Mar. 3, 2015, 2:34 PM), https://tdrt.io/exi. And while "agents can describe the process more fully to a judge in closed chambers," this does not occur unless "the judge knows to ask." Ellen Nakashima, *Meet the Woman in Charge of the FBI's Most Controversial High-Tech Tools*, WASH. POST (Dec. 8, 2015), http://wpo.st/F2022 (attributing the statement to Amy Hess,

footnote continued on next page

4. The risk of foreign prosecution

Most, if not all, network investigative techniques that target foreign computers will violate foreign domestic law, just as foreign-launched cyberexfiltration operations would violate U.S. law,[197] notwithstanding a purported law enforcement purpose.[198] After all, a cyberexfiltration operation originating in the United States that targets a computer in another state is subject to the prescriptive jurisdiction of that state.[199] In 2002, for example, Russia's Federal Security Service filed criminal charges against FBI agents for remotely accessing and extracting data from servers in Chelyabinsk, Russia in order to seize evidence that was later used in a criminal trial.[200] The incident was reportedly "the first FBI case to ever utilize the technique of extra-territorial seizure of digital evidence."[201] The practice largely went underground after this incident, in part "to keep public references to [the FBI's] online surveillance tools to a minimum."[202] The United States, too, has prosecuted foreign state actors for hacking into computers and extracting information. More recently, the DOJ indicted five members of the Chinese military for cyberespionage.[203] The fact that the defendants were likely enforcing Chinese law does not change the fact that their actions violated U.S. law.

---

the head of the FBI's Operational Technology Division, which is responsible for developing and executing the FBI's network investigative techniques, and noting that judges may not really understand what they are authorizing if warrants do not describe techniques in sufficient detail).

197. *See, e.g.*, LVRC Holdings v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009) ("[The Computer Fraud and Abuse Act] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives. . . .'" (second alteration in original) (quoting H.R. REP. NO. 98-894, at 9 (1984))).

198. *Cf.* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 799 (1993) ("'[T]he fact that conduct is lawful in the state in which it took place will not, of itself, bar application of the United States['] . . . laws,' even where the foreign state has a strong policy to permit or encourage such conduct." (first alteration in original) (quoting RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 415 cmt. j (AM. LAW INST. 1987))).

199. *See supra* notes 35-38 and accompanying text.

200. Brunker, *supra* note 42; *see* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

201. Robert Lemos, *Russia Accuses FBI Agent of Hacking*, CNET (Aug. 19, 2002, 5:05 AM PDT) (quoting FBI press release), http://cnet.co/2lRHM6r.

202. *See* Timberg & Nakashima, *supra* note 18 (attributing the statement to former U.S. officials).

203. *See* Press Release, U.S. Dep't of Justice, *supra* note 42.

The DOJ recognizes that cross-border network investigative techniques threaten the sovereignty of other nations. DOJ guidelines for online investigations warn investigators that accessing remotely stored data, or even initiating "personal contact with residents of a foreign state, may violate foreign law. In addition, activity by U.S. law enforcement in such areas may be regarded as a violation of the other nation's sovereignty, creating the potential for serious diplomatic conflict."[204] The Office of the U.S. Attorneys' Criminal Resource Manual cautions that another "nation may regard an effort by an American investigator or prosecutor to investigate a crime or gather evidence within its borders as a violation of sovereignty," including even "seemingly innocuous acts as a telephone call[] [or] a letter."[205]

5. The risk of countermeasures

Affected states that perceive the use of cross-border network investigative techniques as a violation of the United States' international law obligations may seek "self-help" in the form of countermeasures.[206] Countermeasures are "State actions, or omissions, directed at another State that would otherwise violate an obligation owed to that State."[207] Countermeasures must be proportionate to the harm suffered and necessary to compel or convince the violating state to "desist in its own internationally wrongful acts or omissions."[208]

An injured state's right to take countermeasures is triggered by the discovery of a violation of an international norm or treaty obligation

204. ONLINE INVESTIGATIONS WORKING GRP., *supra* note 160, at 16; *see also* CCIPS GUIDELINES, *supra* note 145, at 58 (noting that "issues such as sovereignty and comity may be implicated" in the event investigators access "a computer located in another country" without permission).

205. OFFICES OF THE U.S. ATT'YS, CRIMINAL RESOURCE MANUAL § 267 (1997).

206. *See* Hathaway et al., *supra* note 41, at 857; Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 699 (2014) (detailing how the law of countermeasures applies to cross-border cyberoperations); *see also* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 12 (2011) ("'[R]eciprocal countermeasures'—which have been cited by the U.S. Department of Defense and several scholars as being an effective and even preferable mode of self-help in the cyber context—are deeply problematic for an international legal regime that seeks to appropriately constrain state responses to cyber-conflict." (footnote omitted)).

207. Schmitt, *supra* note 206, at 700. The Draft Articles of State Responsibility codify when and how a state is held responsible for a breach of an international obligation and how a state may respond to international law violations that fall below the threshold of an armed attack or a prohibited use of force. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 56-57 (2001).

208. Schmitt, *supra* note 206, at 700.

attributable to a particular state.[209] Once these requirements are met, the principle of proportionality plays a central role in "modulating the escalation of conflict between states."[210] In the cyber context, "[t]erritorial sovereignty protects cyber infrastructure located on a State's territory, regardless of its governmental character, or lack thereof,"[211] and it may be violated "even when no damage results, as in the case of emplacement of malware designed to monitor a system's activities."[212]

As noted, it is well established that direct exercise of one state's law enforcement functions in the territory of another state requires that state's consent.[213] States that attribute cross-border network investigative techniques to the United States may have a defensible claim that the United States violated customary international law's prohibition on the extraterritorial exercise of law enforcement functions without consent[214] as well as the concomitant principle of nonintervention, which "forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[215] This is particularly the case for attributed law enforcement hacking

209. Hinkle, *supra* note 206, at 16 ("The threshold inquiry for evaluating the legality of countermeasures asks whether there has been (1) an internationally wrongful act that (2) is attributable to another state.").

210. Thomas M. Franck, *On Proportionality of Countermeasures in International Law*, 102 AM. J. INT'L L. 715, 718 (2008); *see* Hinkle, *supra* note 206, at 18-20.

211. Schmitt, *supra* note 206, at 704.

212. *Id.* at 705 (distinguishing such activities from mere espionage or "monitoring," which are permitted); *see also* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. COMPUTER & INFO. L. 347, 352 (2002) (arguing that direct access of foreign-located data "cannot provide the conceptual basis for approaching the legal issues involved in transborder searches and seizures because it would inevitably allow the victim state to transgress upon another state's sovereignty by searching and seizing property belonging to that state's citizens, property that is physically located within that state's territorial boundaries").

213. *See supra* notes 121-29 and accompanying text; *see also, e.g.*, Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117, 171 (1997) ("Enforcement measures requiring consent include not only the physical arrest of a person, but also, for example, service of subpoena, orders for production of documents, and police inquiries.").

214. *See* Bellia, *supra* note 35, at 77 n.143 (concluding that cross-border cyberexfiltration operations violate customary international law based on "the notion that a foreign country's manipulation of data is akin to a trespass and to interference with protected privacy interests"). *But see* Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI. LEGAL F. 103, 108 (arguing that logging on to a remote server after lawfully acquiring a target's password credentials is territorially "ambiguous" and may therefore be in compliance with customary international law).

215. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 205, at 107-08 (June 27); *see* Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 35 (Apr. 9).

operations that move forward with a search after the initial intrusion despite learning that the target is located overseas. Interference with property interests distinguishes network investigative techniques from other forms of espionage, such as the use of spy satellites, where State *A*'s personnel and instruments are anchored in a jurisdictionally neutral territory (for example, outer space) and therefore do not violate the territorial integrity of State *B*.[216]

A review of applicable treaties and diplomatic communications reveals that no state has consented to the United States' launch of cross-border network investigative techniques. In fact, the only multilateral agreement to address the issue of law enforcement "remote access" directly—the Council of Europe's Convention on Cybercrime (Budapest Convention)—explicitly refused to authorize remote cross-border searches.[217] As Oona Hathaway noted, the Budapest Convention may "limit the extent to which parties to the Convention could conduct cyber-attacks against other state parties, since that would undermine the overall intent of the agreement."[218] In 1995, Council of Europe ministers tasked with considering the legal implications of cross-border network investigative techniques recommended against the practice.[219] Experts commissioned in 2009 by the Council of Europe's Project on Cybercrime explained:

> The Recommendation reflects the common understanding of the drafters that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state

216. *See* Bellia, *supra* note 35, at 77 n.143 ("[I]nterference with property interests—as well as personal privacy interests—distinguishes a remote cross-border search from other activities, such as the use of satellites for remote sensing related to management of natural resources and environmental protection, that are not thought to violate international law.").

217. *See* Convention on Cybercrime, *opened for signature* Nov. 23, 2004, S. TREATY DOC. NO. 108-11 (2006), 2296 U.N.T.S. 167 (entered into force July 1, 2004) [hereinafter Budapest Convention]. The Budapest Convention was ratified by the U.S. Senate in September 2006. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL EUR., https://go.coe.int/Be71y (last visited Apr. 4, 2017).

218. Hathaway et al., *supra* note 41, at 864.

219. Comm. of Ministers, Council of Eur., Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (1995), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76. Duncan Hollis has argued that the Budapest Convention's drafters may have purposefully left open provisions concerning cyberattacks by law enforcement. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1052 (2007).

> concerned, and therefore cannot be undertaken without prior consent of the State concerned.[220]

The use of countermeasures to respond to a cyberattack is illustrated by the U.S. response to North Korea's hack of Sony. After the attacks on Sony, President Obama made a public statement that the United States would "respond proportionately" to the incident, calling it an act of cybervandalism.[221] Just days later, the North Korean Internet experienced outages for about ten hours.[222] Many, including North Korea, speculated that the United States was behind a hack that resulted in the outages.[223] That day, Marie Harf, a State Department spokeswoman, told reporters, "We aren't going to [publicly] discuss . . . operational details about the possible response options. . . . [A]s we implement our responses, some will be seen, some may not be seen."[224]

Further complicating the matter is the lack of consensus among states as to how to classify cross-border cyberoperations. As Matthew Waxman notes, "[i]t is widely believed that sophisticated cyber attacks could cause massive harm—whether to military capabilities, economic and financial systems, or social functioning—because of modern reliance on system interconnectivity."[225] And because states differ in how they interpret the application of international norms to harmful cyberoperations, "there is a range of reasonable interpreta-

220. *See* Henrik W.K. Kaspersen, Cybercrime and Internet Jurisdiction 26 (2009), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7 (explaining that the use of processing capacity or data stored on computer systems in a state encroaches on that state's territorial sovereignty, despite uncertainty as to whether cross-border activity in the form of mere communication, such as via telephone, violates territorial sovereignty). In light of this concern, the Convention's drafters agreed to allow direct unilateral cross-border access to data only when those data were generally accessible or when explicit consent was obtained from the data's owner or custodian. *See* Budapest Convention, *supra* note 217, art. 32. In this sense, article 32 is "a permissive rule derived from international custom or from a convention." *See* S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 19 (Sept. 7).

221. David Jackson, *Obama: We're Not at Cyberwar with North Korea*, USA TODAY (Dec. 21, 2014, 1:17 PM EST), http://usat.ly/16FuBL2.

222. *See* Brian Fung, *North Korea's Internet Outage Was Likely the Work of Hacktivists—But Not the Ones You Might Think*, WASH. POST (Dec. 23, 2014), https://wpo.st/6dwd2.

223. *See* Jack Kim, *North Korea Blames U.S. for Internet Outages, Calls Obama "Monkey,"* REUTERS (Dec. 28, 2014, 2:40 AM EST), http://reut.rs/1EwYeNF; *see also* Ashley Feinberg, *So Who Shut Down North Korea's Internet?*, GIZMODO (Dec. 23, 2014, 3:50 PM), http://gizmodo.com/so-who-shut-down-north-koreas-internet-1674589139.

224. *See* Nicole Perlroth & David E. Sanger, *North Korea Loses Its Link to the Internet*, N.Y. TIMES (Dec. 22, 2014), https://nyti.ms/1ARmSCL. A week later the United States placed sanctions on three organizations and ten individuals associated with the North Korean government. *See Sony Cyber Attack: North Korea Calls US Sanctions Hostile*, BBC NEWS (Jan. 4, 2015), http://www.bbc.com/news/world-asia-30670884.

225. Matthew C. Waxman, *Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions*, 89 INT'L L. STUD. 109, 109 (2013).

tions of cyber 'armed attacks' for the purposes of triggering militarily forceful self-defense, and a stable consensus is unlikely for the foreseeable future."[226]

The U.S. position on the use of force in cyberspace incorporates the "scale and effects" test, which focuses on the consequences of a cyberoperation.[227] While this is the most widely held view,[228] a competing position turns on the status of the target and privileges "critical infrastructure" with special protected status.[229] Yet another position turns on the "instrumentality theory," where "[t]he more analogous a new weapon is to conventional forms of military force, the more likely its operation will constitute a 'use of force' or 'armed attack.'"[230]

According to the Senate Armed Services Committee,

> experts agree that gaining access to a target for intelligence collection is tantamount to gaining the ability to attack that target. If a penetration were detected,

---

226. *Id.* at 120-21. Testifying before the Senate Committee considering his nomination to lead the NSA and United States Cyber Command, Michael Rogers explained:

> As a matter of law, DoD believes that what constitutes a use of force in cyberspace is the same for all nations, and that our activities in cyberspace would be governed by Article 2(4) of the U.N. Charter the same way that other nations would be. With that said, there is no international consensus on the precise definition of a use of force, in or out of cyberspace. Thus, it is likely that other nations will assert and apply different definitions and thresholds for what constitutes a use a [sic] force in cyberspace, and will continue to do so for the foreseeable future.

Advance Questions for Vice Admiral Michael S. Rogers, USN: Nominee for Commander, United States Cyber Command 11-12 (2014) [hereinafter Advance Questions], http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf. For an extensive discussion of the debate surrounding the definition of "force" and "armed attack" in Articles 2(4) and 51 of the U.N. Charter, see generally Waxman, *supra* note 41, at 431-37.

227. As Michael Rogers explained:

> DoD has a set of criteria that it uses to assess cyberspace events. As individual events may vary greatly from each other, each event will be assessed on a case-by-case basis. While the criteria we use to assess events are classified for operational security purposes, generally speaking, DoD analyzes whether the proximate consequences of a cyberspace event are similar to those produced by kinetic weapons.

Advance Questions, *supra* note 226, at 11.

228. *See* Hathaway et al., *supra* note 41, at 847 ("Steering a middle course between the instrument- and target-based views, the effects-based approach is the most promising and most widely accepted approach.").

229. One problem with this "target-based" approach is that states define "critical infrastructure" in different ways. *See* TENACE, CRITICAL INFRASTRUCTURE PROTECTION: THREATS, ATTACKS AND COUNTERMEASURES 5-8 (2014), http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf (distinguishing between definitions in the European Union and in the United States); *cf.* Waxman, *supra* note 41, at 436 (discussing the target-based approach).

230. Reese Nguyen, Comment, *Navigating* Jus ad Bellum *in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1117 (2013).

> the victim may not know whether the purpose of the activity would be limited to espionage only, or would also constitute preparation for an attack.[231]

This, coupled with the doctrinal uncertainties described above, may increase the risk of escalation by victim states under the purported justification of anticipatory self-defense, upon a (mistaken, though defensible) fear of an attack in the proximate future. It is for this reason that when Rogers was asked if there were classes of overseas targets that should be "'off-limits' from penetration through cyberspace,"[232] he explained that "the U.S. Government should only conduct cyberspace operations against carefully selected foreign targets that are critical to addressing explicitly stated intelligence and military requirements, as approved by national policymakers and the national command authority."[233]

This appears to directly clash with the use of cyberoperations to collect evidence in pursuit of a criminal actor. Consider a case from 2012 in which an FBI agent applied for and received a warrant to use network investigative techniques to target a suspect believed to be a member of the Iranian military located in Iranian territory.[234] Due to a software malfunction, "the program hidden in the link sent to [the target] never actually executed."[235] But what if the malfunction caused harm to the target computer? Or worse, what if the program executed successfully but allowed the Iranians to match its forensically obtained digital signature to malware used in other, more hostile attacks that were *then* attributed to the United States? In either case, it would be defensible for an adversary state to respond.

The inherent unreliability of malware adds to the risk of escalation. Malware functionality is inherently buggy, and malfunction may lead to harmful, irreversible consequences and collateral damage associated with its

231. *See* Advance Questions, *supra* note 226, at 12 (bolding omitted).

232. *Id.* at 13 (bolding omitted).

233. *Id.*

234. *See* Timberg & Nakashima, *supra* note 18 (noting that a photo e-mailed by the suspect to investigators "appeared to show an olive-skinned man in his late 20s, wearing what court documents described as an 'Iranian tan camouflaged military uniform,'" and that the IP address used to register the e-mail address years prior suggested he was in Tehran, Iran). The suspect "allegedly threatened to detonate bombs at a county jail, a DoubleTree hotel, the University of Denver, the University of Texas, San Antonio International Airport, Washington-Dulles International Airport, Virginia Commonwealth University and other heavily used public facilities across the country." *Id.* The investigators executing the warrant used a spear phishing technique and sent an e-mail containing a link that, when clicked, would cause surveillance software to be downloaded on the target machine. *Id.*; *see supra* note 108 and accompanying text (describing spear phishing techniques).

235. *See* Timberg & Nakashima, *supra* note 18 (quoting a handwritten note from the FBI agent to the court).

use.[236] For example, "[p]oorly designed malware could cause the destruction of data or the corruption of the whole operating system."[237] This is only exacerbated by the Internet of Things phenomenon and the potential security risks of using interconnected devices such as smart light bulbs, connected cars, smart fridges, wearables, and other home security systems.[238] The FBI highlighted this very issue in a 2015 public service announcement about the safety risks associated with the Internet of Things, warning that lack of consumer awareness as to the threat exposure may allow attackers to execute online attacks, resulting in a number of risks, including *physical* harm to consumers.[239]

III. Toward a Normative Legal Process

With the advent of network investigative techniques on the dark web, it has become clear that the criminal legal process should be adjusted to ensure that it better regulates government conduct that has an impact on U.S. foreign relations or national security. Rather than wait for political fallout as a precondition for government intervention,[240] a more forward-looking approach would reallocate decisionmaking authority to institutions better suited to identify and balance foreign relations risks against the law enforcement benefits of using cross-border network investigative techniques.[241]

This raises three fundamental regulatory questions: First, which institutions should set these preferences and calibrate them as the government moves forward within a complex and unpredictable global cybersecurity land-

236. RONALD J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE 25, 31-32 (2013); Mark Mekow & Lakshmikanth Raghavan, *Security Testing of Custom Software Applications*, CSO (July 28, 2010, 8:00 AM PT), http://www.csoonline.com/article/2125378/application-security/security-testing-of-custom-software-applications.html; Quinn Norton, *Everything Is Broken*, MEDIUM: MESSAGE (May 20, 2014), https://medium.com/message/everything-is-broken-81e5f33a24e1#.oc3f76k26.

237. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R44547, DIGITAL SEARCHES AND SEIZURES: OVERVIEW OF PROPOSED AMENDMENTS TO RULE 41 OF THE RULES OF CRIMINAL PROCEDURE 9 (2016).

238. *See Internet of Things Poses Opportunities for Cyber Crime*, FED. BUREAU INVESTIGATION (Sept. 10, 2015), https://www.ic3.gov/media/2015/150910.aspx.

239. *Id.*

240. *Cf.* NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY 30-34 (1994) (noting that law and economics analysis tends to precondition government intervention on regulatory failure to satisfy efficiency benchmarks).

241. *See* Rubin, *supra* note 49, at 469 ("A more comprehensive institutional comparison might consider other goals . . . .").

scape?[242] Second, what policy preferences can be set (using direct and indirect government intervention) to mitigate the immediate risks caused by the failure of the existing rules? Third, how should the policy preferences be implemented and enforced, considering the comparative institutional failures of the existing system?[243]

This Part begins to answer these questions and in doing so outlines a preliminary legal process for managing network investigative techniques. First, it conducts a comparative institutional analysis and concludes that the executive branch is best suited to assume primary responsibility for future government hacking policy. It proposes an interagency conflict resolution scheme to ensure law enforcement hacking policy decisions do not offend foreign relations or national security interests. Second, it sets out baseline policy preferences that constrict the scope of hacking power delegated to the rank-and-file officers executing this new surveillance technique. Third, it lays out a regulatory scheme for implementation and enforcement that involves "a complex, dynamic interaction of institutions that simultaneously work together, challenge each other, defend themselves and divide responsibility."[244] The objective is to enhance the ability to produce decision rules that are predictably and objectively applied, democratically legitimate, and in the overall public interest.[245]

A. Failure of the Existing Legal Process

To be sure, responsibility for the existing system's failure does not lie with *institution-wide* incompetence on the part of the executive branch with respect to foreign relations. The existing system fails because it authorizes rank-and-file officials to make decisions that have direct foreign policy implications

242. Stated another way, which institutions should set rules that balance law enforcement interests against countervailing foreign relations interests? *See id.* at 469 & n.25 ("Law and economics has framed the regulatory debate as an institutional comparison; the operative question is not how well the market functions, but whether the regulatory system could produce a better outcome." (citing RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW (2d ed. 1977))).

243. *See* Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 297 (2011) (calling these "second-order" design choices for enforcing "first-order" preferences).

244. Rubin, *supra* note 49, at 467; *see* Edward L. Rubin, *The New Legal Process, the Synthesis of Discourse, and the Microanalysis of Institutions*, 109 HARV. L. REV. 1393, 1396 (1996) [hereinafter Rubin, *New Legal Process*]; *see also* Daniel B. Rodriguez, *The Substance of the New Legal Process*, 77 CALIF. L. REV. 919, 952 n.177 (1989) (book review) (arguing that "[t]he core insight of legal process is that [policy solutions] will emerge from the synergies associated with the process itself" rather than from substantive law).

245. *See* Rubin, *New Legal Process*, *supra* note 244, at 1414-16 (calling these the most accepted goals for rules).

without meaningful guidance or oversight.[246] This Subpart articulates an executive interagency decisionmaking framework that maximizes information, expertise, coordination, and the ability to make decisions on the fly.

As noted, courts are constrained by the territoriality of warrant authority,[247] broad deference to law enforcement on investigatory matters,[248] and broad deference to the executive branch on matters of foreign policy,[249] particularly in the face of statutory silence or ambiguity.[250] In addition, magistrate judges lack subject matter expertise regarding complex computer science questions and are therefore ill equipped to scrutinize search warrant applications that involve such technologies.[251]

The gap between DOJ policy and DOJ action may also suggest that rank-and-file officers, as opposed to the overarching executive branch, lack subject matter expertise in computer network security and international cyberspace law.[252] Stated another way, rank-and-file officers may not be properly implementing current executive branch policy for cross-border searches because they lack the requisite expertise to realize current policy is applicable in the first place.

---

246. *See supra* Part II.B.

247. *See supra* Part II.A.

248. *Cf.* Rachel A. Harmon, *The Problem of Policing*, 110 MICH. L. REV. 761, 776 (2012) (noting that courts are deferential to law enforcement in part because they recognize their own limited institutional competence). *But cf.* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 587-88 (1952) ("In the framework of our Constitution, the President's power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker.").

249. *See* Curtis A. Bradley, Chevron *Deference and Foreign Affairs*, 86 VA. L. REV. 649, 651 (2000) ("Courts have given deference to the executive branch in foreign affairs matters throughout the nation's history . . . ."); Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1337 (1988) ("The courts have too readily read [United States v.] Curtiss-Wright [Exp. Corp., 299 U.S. 304 (1936),] as standing for the proposition that the Executive deserves an extra, and often dispositive, measure of deference in foreign affairs above and beyond that necessary to preserve the smooth functioning of the national government." (italics omitted)).

250. *See* Chevron U.S.A. Inc. v. Nat. Res. Def. Council, Inc., 467 U.S. 837, 842-43 (1984). Scholars disagree regarding the extent of the deference owed the executive branch in the context of ambiguous statutory authority, but there is no disagreement that some deference is required. *See supra* note 159.

251. *See supra* note 196.

252. *See* Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1411-12 (2009) ("Superior access to information or expertise contributes nothing to accuracy, after all, unless the decisionmaker actually exploits them, and does so reliably."); *see also id.* at 1411 n.168 (citing RICHARD S. MARKOVITS, MATTERS OF PRINCIPLE: LEGITIMATE LEGAL ARGUMENT AND CONSTITUTIONAL INTERPRETATION 217 (1998) (arguing that institutional expertise should be given less weight where the officials "did not actually investigate despite their capacity to do so")).

The executive branch—as a whole—has a comparative institutional advantage over Congress and the federal courts in terms of making foreign policy decisions that turn on rapidly changing technologies. Executive agencies such as the DOJ, the State Department, and the NSA arguably have superior systematic access to information and expertise on both foreign relations and technology—whether through their own subject matter experts[253] or access to other executive agencies that specialize in foreign policy, intelligence gathering, and technology capabilities.[254] By pooling administrative resources, the executive can configure a policymaking team that brings together information and expertise related to foreign relations, law enforcement, technology, and cybersecurity.[255]

An executive agency implementation scheme also has the advantage of being able to adapt in response to rapidly changing technologies and the uncertainties of international norm development. By using executive instruments to set substantive policy preferences, there is minimal cost of changing policy, facilitating a dynamic, nimble policy regime.[256] For example, the DOJ can more easily centralize on-the-fly decisionmaking and provide notice through the rulemaking process and a variety of other administrative

253. *See* William S. Dodge, *Extraterritoriality and Conflict-of-Laws Theory: An Argument for Judicial Unilateralism*, 39 HARV. INT'L L.J. 101, 160 (1998) ("It seems clear that the political branches are institutionally better equipped than courts to reach agreement with other nations about how international business should be regulated."); Koh, *supra* note 249, at 1336 (noting courts' lack of expertise and suggesting structural solutions, including centralization of the adjudication of national security claims in a particular court such as the U.S. Court of Appeals for the District of Columbia Circuit); Julian Ku & John Yoo, Hamdan v. Rumsfeld*: The Functional Case for Foreign Affairs Deference to the Executive Branch*, 23 CONST. COMMENT. 179, 199-201 (2006) (describing how the executive branch's institutional competence in foreign relations is superior to that of the judiciary); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 280-83 (2012).

254. *Cf.* Ku & Yoo, *supra* note 253, at 195-201 ("[C]ourts have access to limited information in foreign affairs cases . . . .").

255. The team should include the Cyber Coordinator, the NSA's representative for the vulnerability equities process, and representatives from the DOJ's CCIPS and OIA.

256. *See* Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2318 (2006) ("And in contrast to the doubters of the unitary executive, I believe a unitary executive serves important values, particularly in times of crisis. Speed and dispatch are often virtues to be celebrated."); *see also* Elena Kagan, *Presidential Administration*, 114 HARV. L. REV. 2245, 2331-46 (2001).

mechanisms.[257] The DOJ also has the capacity to generate uniform rules "and to publicize those rules as binding upon the entire nation."[258]

By contrast, Congress and the courts tend to be sluggish or nonuniform in their decisionmaking.[259] The courts can examine changing issues on a case-by-case basis, but their system of precedent and jurisdictional limitation slows the generation of decision rules that have a uniform national application. And while Congress is able to promulgate laws uniformly, it has not passed a comprehensive electronic surveillance law in over thirty years.[260]

On the other hand, when an institution "makes a major policy move on its own" without sufficient basis in legislative authorization, as it seems the DOJ has done with network investigation techniques, "it undercuts the democratic legitimacy of statutes."[261] The use of cross-border network investigative techniques undercuts the DOJ's democratic legitimacy to the extent it requires an interpretation of its statutory investigative authority to extend overseas, allowing rank-and-file officials to conduct cross-border investigative activities in violation of customary international law, without more explicit authorization from Congress.[262]

Thus, if the executive were to allot broad discretion to rank-and-file officials to shape foreign policy as a matter of course in the execution of search warrants, it would be more consistent with democratic goals to pass the policy

257. William N. Eskridge Jr., *Expanding* Chevron*'s Domain: A Comparative Institutional Analysis of the Relative Competence of Courts and Agencies to Interpret Statutes*, 2013 WIS. L. REV. 411, 419 ("[A]gencies have a variety of mechanisms that allow them to generate national rules relatively quickly: administrative rulemaking, published guidances, handbooks, and even online websites.").

258. *Id.*

259. *Id.* (arguing that case-by-case adjudication is slow); David Alan Sklansky, *Two More Ways Not to Think About Privacy and the Fourth Amendment*, 82 U. CHI. L. REV. 223, 227 (2015) ("And while statutes theoretically can be revised at any time, without waiting for the proper case to arise and without regard for precedent, in practice Congress is often notoriously sluggish.").

260. *Cf.* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522 (2015)).

261. *See* Eskridge, *supra* note 257, at 436.

262. Such an interpretation of statutory authority runs against *the executive's own interpretation* of FBI authority to override customary international law in extraterritorial law enforcement activities. That interpretation requires "direction of the President or the Attorney General" for the FBI to "use its statutory authority" to "investigate and arrest individuals for violations of applicable United States law" if "those actions depart from customary international law." Auth. of the FBI to Override Int'l Law in Extraterritorial Law Enf't Activities, 13 Op. O.L.C. 163, 183 (1989). *But cf.* Extraterritorial Apprehension by the FBI, 4B Op. O.L.C. 543 (1980) (finding no authority for the FBI to conduct cross-border abductions of noncitizens in violation of customary international law).

modification through Congress before it became law.[263] Instead, the executive should adopt the narrower scope of baseline law enforcement hacking capabilities articulated in Part III.B below, which constrain the broad hacking powers the FBI currently has without undermining immediate investigatory goals.

Expansion of law enforcement hacking powers from the baseline preferences should balance law enforcement interests with competing foreign relations and national security interests. One way to do this might be to characterize the problem as a horizontal agency conflict between the DOJ, the NSA, and the State Department. Notwithstanding details of the institutional design solution, the resolution of this conflict should ideally "take advantage of the ability of adversarial relationships to foster fuller development of information and debate, along with broader representation for conflicting interests."[264] To that end, it should entail three things: First, it should balance interests and resolve the conflict. Second, it must generate and promulgate two types of information: (a) information about each agency's policies and (b) information about technical facts. Third, it must generate a record of this information.

That being the case, there are several mechanisms the executive can use.[265] The President can, for example, direct the agencies to negotiate a Memorandum of Understanding (MOU) on interagency protocols that the FBI must follow (for example, decisions must be made under the advisement of the President).[266] The President can, alternatively, create an interagency task force that makes recommendations on law enforcement hacking policy. The President can task the White House Cybersecurity Coordinator with leading a

263. *See* Katyal, *supra* note 256, at 2317 ("[T]he Founders assumed that massive changes to the status quo required legislative enactments, not executive decrees."). As Eskridge has noted, "[s]uch usurpation, even for the best of reasons, is inconsistent with the democratic premises of Article I, Section 7: major policy decisions need to pass through both chambers of Congress and, usually, the President before they become the law of the land." Eskridge, *supra* note 257, at 436.

264. *See* Daniel A. Farber & Anne Joseph O'Connell, *Agencies as Adversaries*, 105 CALIF. L. REV. (forthcoming 2017) (manuscript at 23) (on file with author).

265. *See id.* (manuscript at 24-27) (discussing three forms of interagency conflict resolution mechanisms: resolution through negotiation, resolution through executive adjudication, and resolution through formal voting and consensus rules).

266. *See id.* (manuscript at 24) (citing examples of MOUs between agencies); *see also* Daphna Renan, *Pooling Powers*, 115 COLUM. L. REV. 211, 213-14 (2015) (describing an MOU between the NSA and the DHS "that brings the NSA's technical prowess to bear on DHS-led efforts to secure [domestic] critical infrastructure," allowing the DHS to "achieve cybersecurity objectives that, as a practical matter, would otherwise be unobtainable").

council composed of a high-ranking member of each agency.[267] These decisionmaking frameworks maximize information, expertise, coordination, and the ability to make decisions in response to a rapidly shifting global cybersecurity terrain.

B. Substantive Policy Preferences

This Subpart prescribes substantive restrictions to deal with the immediate risks posed by cross-border network investigative techniques. It identifies three areas where regulation may provide solutions to the new facts of network investigative techniques and proposes standards that balance law enforcement interests against foreign policy interests. To that end, the following substantive policy preferences are not in and of themselves meant to set the normative thresholds for the use of network investigative techniques.[268] Rather, the restrictions are meant to provide a "baseline" from which the executive can craft policy decisions that balance the law enforcement interest in solving criminal cases against the foreign policy and national security interests of the United States. The overriding goal in prescribing them is to minimize the risks outlined in Part II.C above, leaving open the possibility for diplomatic overtures, without forgoing the pressing investigatory needs of locating criminal actors on the dark web.

1. What hacking techniques should be authorized?

A search warrant broadly permits investigators to "use remote access to search electronic storage media and to seize or copy electronically stored information."[269] There is no discernable limit to the range of hacking activities a warrant authorizes. The scope of information that may be collected from

267. This representation is meant to articulate a balance among law enforcement, national security, and diplomatic interests. Of course, the President can add members to this committee or modify their roles. For example, the process can be made more autonomous, in that decisions to expand the government's cross-border hacking policies can be made by a two-thirds vote of the committee, which would ensure balance between law enforcement interests and those of foreign policy and national security. A requirement that the Attorney General sign off on policy changes would allow the DOJ to effectively veto changes that reduce law enforcement hacking capabilities below the baseline policy preferences described in Part III.B below.

268. The normative goal of these "baseline" prescriptions is thus to facilitate prospective policymaking by minimizing the potential harm that rank-and-file decisions can cause to the negotiation processes integral to soft and hard harmonization efforts, the risk of retaliation by other nations, and potential disclosure conflicts between law enforcement and the intelligence community. Importantly, the following policy preferences are not meant to set a "ceiling" on government hacking powers but rather a "floor" from which policy can flow.

269. *See* FED. R. CRIM. P. 41(b)(6).

foreign-located devices by law enforcement can be limited to location information, unless consent is provided from the host nation or custodian of the target device.[270] Such a modification to the scope of law enforcement hacking power satisfies the central investigatory goal of "locating" the target computer while minimizing the interference with the foreign state's sovereignty.[271]

In most cases, country information can be deciphered from IP address information and then used to determine whether the investigation should move forward. If the investigation target is domestic, investigators can proceed with more intrusive means. If the target ends up being overseas, the investigator can initiate the existing diplomatic protocols for cross-border collection of digital evidence, such as the MLAT process.[272] This solution would direct agents to make reasonable efforts to determine the location of digital evidence being remotely collected and to proceed using diplomatic protocols in the event it becomes known during the course of a search that the data are located overseas. It complies with the DOJ's current implementation guidelines and is therefore predictable.[273]

---

270. This rule would comply with norms set by the Budapest Convention. *See* Budapest Convention, *supra* note 217, art. 32 (permitting cross-border access to stored computer data if the data are publicly available or if law enforcement has first obtained consent from the owner of the device). This rule would also comply with U.S. electronic surveillance laws. *See* 18 U.S.C. § 2511(2)(d) (2015); United States v. Barone, 913 F.2d 46, 49 (2d Cir. 1990) (permitting the recording of a conversation between A defendant and a government informant, provided the government obtains the informant's consent and cooperation); Shefts v. Petrakis, 758 F. Supp. 2d 620, 630 (C.D. Ill. 2010) (noting that the collection of e-mails and text messages is permitted with consent).

271. Collection of publicly available port information does not infringe international law. *See* Budapest Convention, *supra* note 217, art. 32. Moreover, a solution that only returns country information is of sufficiently low intensity that proportionate responses by injured states are unlikely to be prohibitive. *See supra* notes 227-35 and accompanying text.

272. *See supra* Part I.B.

273. *See* ONLINE INVESTIGATIONS WORKING GRP., *supra* note 160, at 64 ("[A]gents should always make reasonable efforts to find out where the relevant electronic records are stored. If they learn before or during the search that the information may be stored in servers outside the United States, they must proceed as they would to obtain physical evidence located outside the U.S. If agents later discover they have inadvertently downloaded information from servers located abroad, they should seek immediate guidance from those authorities within their agencies who handle obtaining evidence from foreign nations.").

2. Who should be targeted?

The Federal Rules of Criminal Procedure allow investigators to search and seize the property of nonsuspects.[274] International law, on the other hand, requires a proper prescriptive basis—some nexus between the search target and the harmful local effects that spawned the investigation in the first place—before a state may exercise any form of extraterritorial jurisdiction.[275]

Operationally, the use of network investigative techniques risks hacking foreign-located computers that belong to innocent people. One potential baseline policy preference that strikes the balance is to require investigators to make a showing of *target* culpability—for example, that the target device is owned or controlled by a criminal suspect or a fugitive.[276] Another way to strike this balance is to limit the use of cross-border network investigative techniques to the collection of items whose mere possession violates U.S. law.[277] These limiting principles minimize the situations where the United States asserts jurisdiction over a foreign-located noncitizen who has not caused effects in the United States, thus making cross-border network investigative techniques more defensible to the international community.

3. What crimes should trigger use of hacking techniques?

Another factor that will likely affect how states react to encroachments on their sovereignty that result from cross-border network investigative techniques is the seriousness of the crime being investigated. As noted, international norms in cyberspace are in development and likely to emerge as a result of state practice. The DOJ has made it clear that it intends to use hacking techniques for all crimes, regardless of the potential cross-border implications.[278]

---

274. *See* FED. R. CRIM. P. 41(c) (providing that a warrant may issue for "evidence of a crime," "contraband . . . or other items illegally possessed," or "property designed for use, intended for use, or used in committing a crime").

275. *See supra* notes 35-38 and accompanying text (describing the effects test for prescriptive jurisdiction).

276. *Cf.* United States v. Grubbs, 547 U.S. 90, 96 (2006) ("Anticipatory warrants are, therefore, no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed.").

277. Network investigative techniques that infect computers that visit a particular child pornography server are particularly effective in sting operations because anyone who knowingly accesses the server is committing a crime. *See* Memorandum from Jonathan J. Wroblewski, Dir., Office of Policy & Legislation, Criminal Div., U.S. Dep't of Justice, to Judge John F. Keenan, Chair, Subcommittee on Rule 41, Advisory Comm. on Rules of Criminal Procedure (Jan. 17, 2014), *in* ADVISORY COMM. ON CRIMINAL RULES, *supra* note 25, at 179, 180, 205-06.

278. *See id.*

The DOJ's position would make it defensible for foreign law enforcement actors to hack computers in the United States as long as those actors are in investigatory pursuit of a violation of that foreign nation's criminal laws. This is a policy decision that should benefit from the experience and expertise of other agencies and consideration of U.S. foreign relations and national security implications.

There are several ways to reduce the scope of crimes that trigger the use of hacking techniques. One baseline policy preference might limit the use of network investigative techniques to counterterrorism investigations, for which—at least under the United States' interpretation of international law—extraterritorial enforcement is grounded in conceptions of self-defense.[279]

Another limiting principle that would likely be defensible with U.S. allies in the international community is one that tailors the use of network investigative techniques to the pursuit of crimes whose seriousness is broadly acknowledged by states, such as terrorism, child pornography offenses, drug crimes, and organized cybercrime.[280] Indeed, there is a history of coordination among the Group of Eight (G8) countries with regard to regulating these crimes.[281] For these reasons, cross-border action limited to a small set of crimes considered especially heinous will be perceived as more reasonable than an open-ended solution and thus may be more likely to receive the support of the international community.[282] This solution will cause minimal friction with allies, and it is therefore more likely to keep diplomatic channels open.[283]

---

279. The legality of such actions is not always certain. *See* David Kretzmer, *Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?*, 16 EUR. J. INT'L L. 171, 191-97 (2005) (arguing that in international armed conflicts suspected terrorists are not combatants, though in noninternational armed conflicts they may well be combatants, and arguing that the applicable system should incorporate features of both international human rights law and international humanitarian law).

280. *See* Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* 74 (Tilburg Law Sch. Legal Studies Research Paper Series, No. 05/2016, 2014), https://ssrn.com/abstract=2698263.

281. *See* Goldsmith, *supra* note 185, at 147 ("The G8 economic powers have recently begun to coordinate regulatory efforts concerning Internet-related crimes in five areas: paedophilia and sexual exploitation; drug-trafficking; money laundering; electronic fraud, such as theft of credit-card numbers, and computerized piracy; and industrial and state espionage.").

282. *See id.* at 147-48 (suggesting that there will be more cross-border coordination of regulatory efforts in areas where national interests converge).

283. An even less risk-averse approach may allow the use of cross-border network investigative techniques to be triggered by all crimes with extraterritorial application, satisfying the requirements of prescriptive jurisdiction though still subjecting the United States to some level of risk. One advantage of the executive branch promulgating these policy preferences is the ability to create and change policy on the fly. *See supra* note 256. This facilitates a law enforcement policy that is in tune with foreign relations policies on cyberspace, which are largely set by the executive.

C. Implementation and Enforcement

Having selected the institutional actors that should set substantive cross-border hacking policy preferences for law enforcement moving forward, this Subpart turns to the implementation and enforcement of those policies. The existing disparity between DOJ policy and practice suggests a breakdown in implementation and enforcement.[284] This inconsistency "undermines the predictability of law and reverses assumptions upon which private industry and the public sector have reasonably relied."[285]

The judiciary is the traditional regulating institution for criminal procedure.[286] Its neutrality and detachment make it suitable to make the inferences required to grant or deny a warrant[287] in light of the obvious conflict of interest presented by law enforcement's focus on the "often competitive enterprise of ferreting out crime."[288] Ex ante judicial review helps prevent investigators from ignoring or misinterpreting the established legal limits on their authority.[289] Ex post judicial review provides additional checks that incorporate the adversarial process. However, the courts are constrained in their authority to regulate cross-border aspects of network investigative techniques because of warrant authority's territoriality, the compulsion to defer to law enforcement, and judicial deference to the executive in the realm of foreign policy.[290] This leaves Congress as the primary interbranch check on the foreign relations implications of law enforcement hacking.

Congress can influence the legal process in a number of ways without legislating substantively. First, Congress could legislate procedural

284. *See* Katyal, *supra* note 256, at 2318. Jonathan Mayer notes the following implementation problems with network investigative techniques: (1) "[d]escriptions of malware are often ambiguous and misleading," (2) investigators sometimes "assert[] that no warrant is required at all," (3) malware may be delivered to innocent users, (4) "[w]arrant applications [may] ignore . . . the unambiguous[] time limits of Rule 41," and (5) "the government [may] not properly appl[y] for a super-warrant in scenarios where they are unambiguously required." Jonathan Mayer, Constitutional Malware 75 (Nov. 15, 2016) (unpublished manuscript), https://ssrn.com/abstract=2633247.

285. *See* Eskridge, *supra* note 257, at 436.

286. *See, e.g.*, Johnson v. United States, 333 U.S. 10, 14 (1948).

287. *Id.*

288. *Id.* The structure of the Fourth Amendment recognizes the intransigence of this conflict by requiring a neutral disinterested arbiter to make the determination of what is a search and whether the executive has shown probable cause of a crime sufficient to overcome the constitutional privacy interest of the target. *See* U.S. CONST. amend. IV; *Johnson*, 333 U.S. at 14.

289. S. REP. NO. 90-1097, at 97 (1968) ("Judicial review of the decision to intercept wire or oral communications will not only tend to insure that the decision is proper, but it will also tend to assure the community that the decision is fair.").

290. *See supra* notes 247-51.

mechanisms that encourage predictable, objective application of government hacking policies and clear and accountable lines of command within the executive branch. For example, Congress could enact a statutory requirement that any warrant application for the use of network investigative techniques on the dark web must be authorized by the U.S. Attorney General or another designated high-ranking official.[291] Limiting the government actors who may authorize the application for a hacking warrant "centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques."[292] Having high-ranking officials sign off on individual warrants increases the concentration of information and expertise in the decisionmaking process[293] and incentivizes applications only where the circumstances justify them.[294] Such a requirement would avoid the development of divergent practices across the U.S. Attorneys' Offices while providing "lines of responsibility . . . to an identifiable person" in the event of abuse.[295] Additionally, by forcing the agency to absorb some of the costs of violating policy, this solution would incentivize restraint in execution.[296] Congress could also require certifications

291. This requirement would mirror that for applications seeking an order to intercept wire or oral communications, which requires that "[t]he Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division or National Security Division specially designated by the Attorney General" authorize the filing of the application. 18 U.S.C. § 2516(1) (2015) (footnote omitted).

292. S. REP. NO. 90-1097, at 97; *cf.* FED. R. CRIM. P. 41(b) (permitting any federal law enforcement officer or attorney for the government to apply for a search warrant).

293. *See* Joseph Lynch, *Justice Department Procedures for Approval of Wiretapping and Eavesdropping Orders*, CRIM. DEF., Sept.-Oct. 1977, at 11, 11 (providing a description of internal review procedures for the Wiretap Act). The Wiretap Act was first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. *See* Wiretapping and Electronic Surveillance, Pub. L. No. 90-351, tit. III, 82 Stat. 211 (codified as amended at 18 U.S.C. §§ 2510-2522). In 1986, Congress amended the Wiretap Act to extend telephone wiretap restrictions to computer data transmissions. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522).

294. *See* United States v. Giordano, 416 U.S. 505, 515 (1974) (noting in the context of the Wiretap Act that Congress "evinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications"). The DOJ's commentary has rejected any limitations on the scope or manner of execution. *See* Memorandum from David Bitkower to Judge Reena Raggi, *supra* note 155, at 3 (arguing against restrictions on remote search authority).

295. *See* S. REP. NO. 90-1097, at 97 ("This provision in itself should go a long way toward guaranteeing that no abuses will happen.").

296. *See generally* Robert W. Hahn, *The Economic Analysis of Regulation: A Response to the Critics*, 71 U. CHI. L. REV. 1021 (2004) (explaining and defending cost-benefit analysis in regulatory decisionmaking).

to satisfy the judge that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[297] This leverages DOJ expertise in situations where the courts lack appropriate technological expertise to assess whether the target's location has indeed been obscured by technological means.[298]

Second, Congress could exercise oversight powers on federal law enforcement's use of network investigative techniques. Congressional oversight can be implemented through legislative hearings by a standing congressional committee, such as the House Judiciary Committee or the House Intelligence Committee. To bolster the effectiveness of the oversight process, Congress should work to "equaliz[e] its access to sensitive information that otherwise lies solely within the Executive's control" and build centralized technology and foreign affairs expertise within Congress to better analyze that information.[299] This can be done by passing legislation imposing reporting requirements on the scope and nature of permitted hacking techniques, their frequency of use, and instances where foreign-located computers are affected. Hearings should be open to the public to the extent possible, limiting closed sessions to cases where information that is classified or related to an ongoing investigation must be shared with members.

Third, Congress could indirectly regulate the nature and scope of hacking techniques used by investigators through its authority over financial and budgetary matters. Malware is expensive, with prices rising as high as $500,000.[300] By adjusting budget allocations, for example, Congress could indirectly control law enforcement's procurement of malware tools through line item adjustments or by barring the use of funds to procure tools that do not comply with the vulnerability equities process.

Fourth, Congress can allocate resources to bolster the judiciary's technological expertise. The courts will continue to play a key role in regulating network investigative techniques by interpreting and applying constitutional and statutory checks and balances. These functions require, at minimum, an understanding of how the network investigative technique under scrutiny

297. *See* 18 U.S.C. § 2518(3)(c) (requiring such certifications before approving a telephone warrant request). In commentary, the DOJ has rejected such a "necessity requirement." *See* Memorandum from David Bitkower to Judge Reena Raggi, *supra* note 155, at 3.

298. *Cf.* Ctr. for Democracy & Tech., *supra* note 31, at 6-7 (describing various instances when a target's location may be obscured but not in a manner that stifles the use of current investigative techniques).

299. Koh, *supra* note 249, at 1327.

300. *See* Greenberg, *supra* note 172; *see also* Brian Fung, *The NSA Hacks Other Countries by Buying Millions of Dollars' Worth of Computer Vulnerabilities*, WASH. POST (Aug. 31, 2013), https://wpo.st/Qb2e2 (explaining that in 2013 the NSA allocated more than $25 million to purchase malware from private parties).

works. This, in turn, requires a level of technological expertise. To that end, technology training and access to expert assistance when necessary is critical to ensure that judges can ask the right questions and spot irregularities.

Fifth, Congress could legislate mechanisms that encourage adversarial challenges to the legality of network investigative techniques. One way to do this through the courts is to enact an evidentiary suppression sanction for violations in the application or execution of network investigative techniques.[301] This would enable a criminal defendant to challenge the use of evidence obtained from unlawful hacking.[302] Statutory suppression also incentivizes restraint in execution by making law enforcement absorb the cost of a violation.[303] This also invites outside scrutiny of network investigative techniques, which can add valuable technical expertise to the public debate.[304] By ensuring that other institutions and the public have ample opportunities to review the use of this powerful tool, society can ensure that law enforcement has clear incentives to exercise reasonable care when using network investigative techniques.[305]

Conclusion

Law enforcement's use of hacking techniques to pursue criminal suspects on the dark web will result in overseas cyberexfiltration operations that may violate the sovereignty of other nations. The risks associated with such techniques are enormous: disability of U.S. foreign relations, exposure of the United States and its citizens to countermeasures, and exposure of the

301. Statutory suppression of evidence applies in other surveillance contexts. *See* 18 U.S.C. § 2518(10)(a) (providing statutory suppression for persons aggrieved by a violation of the Wiretap Act); *cf.* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 63 (2004) ("[O]nline surveillance, including dynamic content interceptions, lack[s] the statutory suppression remedy that Congress provided for traditional surveillance in the Wiretap Act. . . . The omission is not aligned with a major goal of the [Electronic Communications Privacy Act]—to ensure the privacy of electronic communications and extend all of the Wiretap Act's protections to the new media.").

302. *See* S. REP. NO. 90-1097, at 96 (1968) (noting that in the wiretapping context, "[s]uch a suppression rule is necessary and proper to protect privacy"). A standard that matches the Wiretap Act would allow any aggrieved person—not just those whose devices were breached—to challenge the legality of such evidence, so long as it is being used against her in a trial, hearing, or any other legal proceeding.

303. *See supra* note 296 and accompanying text.

304. One example of outside scrutiny is challenges by technical experts in criminal cases.

305. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 817 (2003) (explaining that wiretaps are subject to more oversight than compelled disclosure of digital evidence under the SCA because the latter lacks a statutory suppression remedy).

investigators performing overseas searches and seizures to prosecution by foreign nations. These circumstances highlight the failures of the existing rules of criminal procedure as applied to the new facts of cross-border network investigative techniques. And they call into question the wisdom of authorizing rank-and-file officials to make enforcement decisions that reverberate globally without any meaningful interagency coordination or interbranch checks and balances.

Criminal procedure must evolve to balance the use of network investigative techniques against countervailing foreign relations interests that may be harmed by unlawful foreign searches. This will require adjustments to the legal process that minimize the risk of political fallout by (1) maintaining existing jurisdictional norms governing the United States' cross-border criminal investigations and (2) implementing structural modifications that allocate critical foreign policy decisions to the government institutions best suited to make them. Only then can network investigative techniques be implemented and enforced in a way that is predictable, legitimate, and in the public interest.