Stanford Law Review Online

Volume 70 July 2017

ESSAY

Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?

Orin S. Kerr* & Sean D. Murphy**

Introduction

Government hacking is everywhere. Hackers working for the Russian government broke into computers run by the Democratic National Committee and stole e-mails relating to the 2016 Presidential election.[1] Hackers traced to the Chinese government broke into U.S. government computers and copied personnel files of over 22 million employees.[2] North Korean hackers intruded into Sony computers in the United States in response to a film that poked fun at North Korea's leadership.[3] The United States and Israel reportedly hacked into Iranian government computers to disable their centrifuges at an Iranian nuclear plant.[4]

But not all government hacking is for purposes of espionage or revenge. In some cases, governments hack into computers as part of legitimate criminal investigations. Ahmed Ghappour's new article, *Searching Places Unknown: Law*

* Fred C. Stevenson Research Professor, George Washington University Law School. The authors thank Ahmed Ghappour, Nathan Judish, and Dave Aitel for commenting on an earlier draft of this response.

** Manatt/Ahn Professor of International Law, George Washington University Law School.

1. *See* Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://nyti.ms/2hBJis3. Or at least that is believed to be the case. Attribution is always difficult in computer intrusion cases.
2. *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), http://wapo.st/1CsdmLU?tid=ss_tw-bottom&utm_term=.27bbf547ff1c.
3. *See* Press Release, FBI National Press Office, Update on Sony Investigation (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.
4. *See* William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), https://nyti.ms/2uDIgOK.

Enforcement Jurisdiction on the Dark Web,[5] focuses on a discrete piece of the government hacking puzzle: legal oversight of United States government hacking used in criminal investigations to search computers located abroad of suspects that use internet anonymizing services such as Tor.[6]

As Ghappour's title indicates, such hacking involves "Searching Places Unknown." Use of anonymizing software conceals the user's location so that investigators cannot know where to begin their investigation. Unless the target slips up, a government's best chance of identifying who is behind the crime and where he is requires tricking the target into downloading malicious code—in the government's generic terminology, a "network investigative technique" or NIT[7]—that searches for location information on the target's computer and sends it to the government. With the suspect's location (and perhaps identity) revealed, the investigation can focus on that location and proceed in the usual way.

Ghappour argues that government use of NITs to investigate users of anonymizing software in criminal cases "presents a looming flashpoint between criminal procedure and international law."[8] In his view, such actions "may violate the sovereignty of other nations."[9] Because the government does not know where the computers to be searched are located, use of the technique might ultimately search computers located abroad. This poses significant foreign relations risks for the United States, Ghappour argues.[10] It may offend foreign nations, might violate customary international law's prohibition on a

5. Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075 (2017).

6. Ghappour's article refers to "the Dark Web" and "the Tor network" interchangeably. *Id.* at 1087 n.50. This terminology is confusing because the phrase "dark web" normally is used to refer only to nonindexed websites that are accessible exclusively through anonymizing services such as Tor. *See* Andy Greenberg, *Hacker Lexicon: What is the Dark Web?*, WIRED (Nov. 19, 2014, 7:15 AM), https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web. Tor and the dark web are therefore different: according to one estimate, only about 2% of Tor traffic is traffic to the nonindexed websites that (as traditionally understood) make up the dark web, and that are widely used for criminal purposes such as to host child pornography. *See* Andy Greenberg, *Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds*, WIRED (Dec. 30, 2014, 12:30 PM), https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds. While every investigation of the dark web involves an anonymizing services such as Tor, not every investigation of users of Tor and similar services involve the dark web.

7. The term "network investigative technique" and its acronym "NIT" has no clear technical meaning. It is simply a bland term the government uses rather than a technical concept. In this response, we assume the term refers to software used to bypass security features controlling access to a computer.

8. Ghappour, *supra* note 5, at 1075.

9. *Id.* at 1135.

10. *Id.* at 1108.

state's extraterritorial exercise of law enforcement functions without consent, and might lead to criminal prosecution of U.S. officials abroad.[11]

This is particularly troubling, Ghappour contends, because United States law imposes no regulatory structure on the use of cross-border NITs to investigate users of anonymizing software.[12] No judicial review is necessary because the warrant requirement does not apply to computers searched abroad.[13] No statute requires internal executive branch oversight.[14] This leaves use of the tool to the complete discretion of "rank-and-file" investigators, operating in a "regulatory vacuum," who are unlikely to understand executive branch policy or to recognize the foreign relations risk of use and misuse of the tools.[15] Ghappour therefore recommends a series of reforms to ensure sufficient executive branch oversight of these new tools.[16]

* * *

Ghappour's article is provocative and interesting, but we are not convinced that a genuine problem exists. This response challenges Ghappour's framework in three ways. First, it questions whether there are real international relations difficulties with the use of NITs to investigate internet users who have used anonymizing software to thwart law enforcement investigations. Second, it questions whether government use of NITs in this context violates international law. Third, it argues that the use of NITs on the dark web does not occur in a "regulatory vacuum."

To be clear, we agree with Ghappour that government use of NITs raises significant technical, legal, and policy challenges. We also agree that, at a broad level of generality, extraterritorial evidence collection over the internet by one nation can in some circumstances offend other nations and violate international law. At the same time, we are unpersuaded that there is a major threat to international relations and international law in the specific context of governments using NITs to circumvent anonymizing software and investigate crimes on the dark web.

11. *Id.* at 1108-22.
12. *Id.* at 1123-28.
13. *Id.* at 1124.
14. *Id.* at 1126.
15. *Id.* at 1108.
16. *Id.* at 1128-35.

I. Does Use of NITs to Investigate Dark Web Cases Threaten International Relations?

Let's start with Ghappour's claim that using NITs to investigate dark web cases raises substantial risks to international relations.[17] We are skeptical. In our view, Ghappour's concerns about the risks of government use of malware to locate users of internet anonymizing services overlook both the pervasive nature of transnational law enforcement cooperation generally and the existing practice of government cooperation and coordination in dark web investigations specifically.

In recent decades, international cooperation in the investigation and enforcement of criminal law has become the norm. A complex web of global, regional, and bilateral treaties now exists addressing a wide range of crimes, such as cybercrime,[18] corruption,[19] transnational organized crime,[20] narcotics,[21] and terrorism.[22] Further, a network of mostly bilateral treaties focuses on extradition[23] and mutual legal assistance[24] for crimes punishable in both jurisdictions. States also cooperate extensively through international

17. *Id.* at 1083-87.

18. *See, e.g.*, Council of Europe, Additional Protocol to the Convention on Cybercrime, Jan. 28, 2003, E.T.S. No. 189; Council of Europe, Convention on Cybercrime, Nov. 23, 2001, S. TREATY DOC. NO. 108-11, E.T.S. No. 185.

19. *See, e.g.*, G.A. Res. 58/4, annex, U.N. Convention Against Corruption (Oct. 31, 2003); African Union Convention on Preventing and Combating Corruption, July 11, 2003, 43 I.L.M. 5; Council of Europe, Criminal Law Convention on Corruption, Jan. 27, 1999, E.T.S. No. 173; Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, Dec. 18, 1997, S. TREATY DOC. NO. 105-43, 37 I.L.M. 1; Organization of American States, Inter-American Convention Against Corruption, Mar. 29, 1996, S. TREATY DOC. NO. 105-39, O.A.S.T.S. NO. B-58.

20. *See, e.g.*, United Nations Convention against Transnational Organized Crime, annexes I (main convention), II (protocol on trafficking in persons), & III (protocol on smuggling migrants), Jan. 8, 2001, S. TREATY DOC. NO. 108-16 (2003).

21. *See, e.g.*, United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, S. TREATY DOC. NO. 101-4, 1582 U.N.T.S. 164; U.N. Convention on Psychotropic Substances, Feb. 21, 1971, 1019 U.N.T.S. 175.

22. *See, e.g.*, Council of Europe, Convention on the Prevention of Terrorism, May 16, 2005, C.E.T.S. No. 196; Organization of American States, Inter-American Convention Against Terrorism, June 3, 2002, S. TREATY DOC. NO. 107-18, 42 I.L.M. 19; International Convention for the Suppression of the Financing of Terrorism, Dec. 9, 1999, S. TREATY DOC. NO. 106-49; International Convention for the Suppression of Terrorist Bombings, *opened for signature* Jan. 12, 1998, S. TREATY DOC. NO. 106-6 (entered into force May 23, 2001).

23. *See generally* DAVID A. SADOFF, BRINGING INTERNATIONAL FUGITIVES TO JUSTICE: EXTRADITION AND ITS ALTERNATIVES 138 (2016) (explaining the law and practice of extradition treaties).

24. *See* ROBERT CRYER ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE 107-10 (3d ed. 2014).

organizations, be it Interpol,[25] the Council of Europe,[26] or the U.N. Commission on Crime Prevention and Justice,[27] or through ad hoc ministerial summits on crime prevention.

Embassies around the world are staffed with persons charged with investigating transnational crimes, often referred to as legal attachés. Transnational telephone calls, faxes, e-mails, and internet searches by law enforcement authorities are ubiquitous; they are no longer limited to the occasional diplomatic note from an embassy to a foreign ministry that may have featured in decades past.[28] In short, governments are no longer surprised at or offended by the idea that criminal conduct within a State's territory is of great interest to other governments, and readily pursue pragmatic cooperation on a reciprocal basis to address transnational threats.

Cooperation among governments is a particularly significant part of computer crime investigations given the borderless nature of the internet. For the last twenty years, the Computer Crime and Intellectual Property Section at DOJ has made international cooperation in the enforcement of computer crimes laws one of its highest goals.[29] It has hosted conferences on the topic,[30] advised Interpol, helped set up the G8 network, and played a leading role in the

25. *See generally* JEAN F. BLASHFIELD, INTERPOL (2004) (explaining transnational law enforcement cooperation through Interpol).

26. For an explanation of transnational law enforcement cooperation through the Council of Europe, see Werner Sipp, *Co-operation Group to Combat Drug Abuse and Illicit Trafficking in Drugs (Pompidou Group)*, *in* THE COUNCIL OF EUROPE: ITS LAW AND POLICIES 413, 413-25 (Stephanie Schmahl & Marten Breur eds., 2017); Wolfgang Rau, *Group of States Against Corruption (GRECO)*, *in* THE COUNCIL OF EUROPE, *supra*, at 444, 444-64; Christian Walter, *Combating Terrorism and Organised Crime*, *in* THE COUNCIL OF EUROPE, *supra*, at 672, 672-95.

27. *See Commission on Crime Prevention and Criminal Justice*, U.N. OFF. ON DRUGS & CRIME, http://www.unodc.org/unodc/en/commissions/CCPCJ/ (last visited July 3, 2017).

28. *See generally* CROSS-BORDER LAW ENFORCEMENT: REGIONAL LAW ENFORCEMENT COOPERATION: EUROPEAN, AUSTRALIAN AND ASIA-PACIFIC PERSPECTIVES (Saskia Hufnagel et al. eds., 2012) (tracking the rise in cross-border cooperation between police and judicial authorities); POLICING ACROSS BORDERS: LAW ENFORCEMENT NETWORKS AND THE CHALLENGES OF CRIME CONTROL (George Andreopoulos ed., 2012) (exploring challenges confronting the law enforcement community in the Balkan region in confronting critical transnational threats); TRUST IN INTERNATIONAL POLICE AND JUSTICE COOPERATION (Saskia Hufnagel & Carole McCartney eds., 2017) (explaining transnational law enforcement cooperation).

29. *See Overseas Work*, U.S. DEP'T OF JUST., COMPUT. CRIME & INTELL. PROP. SECTION (Feb. 10, 2017), https://www.justice.gov/criminal-ccips/overseas-work; U.S. Dep't of Justice, Comput. Crime & Intellectual Prop. Section, International Cooperation in Cybercrime Investigations 5-7 (Feb. 28, 2008), https://www.oas.org/juridico/spanish/cyber/cyb22_coop_handout.pdf.

30. *See, e.g.*, *CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders*, U.S. DEP'T OF JUST., COMPUT. CRIME & INTELL. PROP. SECTION (June 6, 2016), https://www.csis.org/events/ccips-csis-cybercrime-symposium-2016.

Council of Europe Convention on Cybercrime.[31] Enforcing domestic computer crimes means investigating crimes around the globe, and international cooperation has long been an essential part of that picture.

International cooperation is particularly strong in cases that involve large-scale criminal enterprises on the dark web. [32] Such crimes occur on a global scale. Visitors to websites hosted on the dark web use anonymizing technology to hide their locations from international law enforcement authorities. A criminal website on the dark web could be hosted anywhere; visitors are often drawn from all over the world; and those visitors often engage in crimes that are serious felonies in every jurisdiction. And every government is in the same boat, as every government is blocked from successfully investigating by the same technology.

The question is, how have governments responded to the apparent need to use NITs to light the dark web? Ghappour portrays the United States government as using NITs on the dark web to unilaterally invade the sovereignty of other countries to pursue its purely domestic objectives. The more accurate narrative in these cases, it seems to us, is one of international cooperation rather than a threat to sovereignty. One government's use of NITs to investigate crimes on the dark web is generally welcomed by other governments rather than feared.

Consider the Playpen investigation. Playpen was a child pornography website available only on the dark web that had over 100,000 unique user accounts.[33] An NIT installed by the United States pursuant to a warrant ended up searching over one thousand computers in many different countries.[34] That led to further investigations and hundreds of arrests around the world.[35] A presentation by Europol, the European Union's law enforcement agency, suggests that the investigation was international in scope, combining resources in the EU with resources in the United States and Australia.[36] It was an

31. *See* Convention on Cybercrime, *supra* note 18.

32. *See, e.g.*, U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION AND INTERDICTION 16-17 (2016), https://www.justice.gov/psc/file/842411/download.

33. *See* Gabrielle Banks, *Federal Agents Sweep Child Pornography Site by Hacking 'Dark Web' Site*, HOUS. CHRON. (Apr. 10, 2016), www.houstonchronicle.com/news/houston-texas/houston/article/Federal-agents-sweep-child-pornography-site-by-7240097.php.

34. *See* Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, VICE: MOTHERBOARD (Jan. 5, 2016, 1:00 PM), https://motherboard.vice.com/en_us/article/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers; Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, VICE: MOTHERBOARD (Jan. 22, 2016, 11:01 AM), https://motherboard.vice.com/en_us/article/child-porn-sting-goes-global-fbi-hacked-computers-in-denmark-greece-chile.

35. *See* Joseph Cox, *Child Porn Sting Goes Global, supra* note 34.

36. Rob Wainwright, Director, Europol, Combatting Child Sexual Exploitation: The European Approach 4 (2015), https://www.scribd.com/document/296325516/Operation-Pacifier-Powerpoint-Presentation.

international effort to combat a global criminal enterprise. As far as we know, no foreign government has objected to it.

A recent Justice Department report provides another example.[37] More than 200 child pornography websites operating on the Tor network were recently taken down by "a globally coordinated criminal investigation" by "DOJ, FBI, the European Union's Europol agency, and other foreign partners."[38] According to the Report:

> The operational strategy and framework allowed for parallel investigations to be conducted in each participating nation; enhanced efficiency by pooling resources among all participating countries; and recognized that real-time information sharing would—and needed to be—the norm. More than 70 law enforcement agents from the United States, Finland, France, Germany, Greece, Ireland, the Netherlands, Norway, Poland, Spain, Sweden, Switzerland, and the United Kingdom cooperated in the investigation, while Europol served as the hub for operational support, facilities, and information sharing.[39]

The challenge of Tor appears to be triggering increased governmental cooperation rather than raising fears of territorial encroachment.[40]

The Silk Road investigation echoes the point. Silk Road was a global online drug bazaar, available only through Tor, which allowed anyone in the world to purchase illegal items such as narcotics. United States investigators were able to locate the server that hosted Silk Road because the website was misconfigured in a way that revealed its true location.[41] After repeatedly querying the site, they learned that it was hosted in Reykjavik, Iceland.[42] Icelandic authorities then cooperated with the investigation, seizing a copy of the server pursuant to their legal process and handing it over to the FBI.[43]

The absence of United States opposition to foreign government hacking on the dark web is also notable. The United States is not alone in hacking to

---

37. U.S. DEP'T OF JUSTICE, *supra* note 32, at 16-17.

38. *Id.* at 17.

39. *Id.*; *see also* Press Release, U.S. Dep't of Justice, New York Man Sentenced to Six Years in Prison for Receiving and Accessing Child Pornography (Dec. 17, 2015), https://www.justice.gov/opa/pr/new-york-man-sentenced-six-years-prison-receiving-and-accessing-child-pornography (noting 19 convictions of individuals in the United States who visited a child pornography website on the dark web, and noting that Europol assisted in the investigation).

40. *See* U.S. DEP'T OF JUSTICE, *supra* note 32, at 92-93.

41. *See* Joshuah Bearman & Tomer Hanuka, *The Rise & Fall of Silk Road: Part II*, WIRED (June 2015), https://www.wired.com/2015/05/silk-road-2.

42. *See id.*

43. *See id.* According to the government, the Silk Road Investigation did not use an NIT. Some security researchers are skeptical about this assertion. *See, e.g.*, *Silk Road Lawyers Poke Holes in FBI's Story*, KREBS ON SECURITY (Oct. 14, 2014, 7:05 PM), https://krebsonsecurity.com/2014/10/silk-road-lawyers-poke-holes-in-fbis-story. Either way, the Silk Road investigation helps show the norm of international cooperation to solve cases involving the dark web.

light the dark web. Other countries do it, too.[44] Europol recently used an NIT to search the computers of visitors to a dark web child pornography site called The Giftbox Exchange.[45] The Australian government recently used a phishing attack to hack the computers of visitors to a dark web child pornography site called The Love Zone.[46] In at least one known instance, the Australian government hacking broke into computers in the United States.[47] There is no sign that the United States government or the American public was offended by the foreign search. To the contrary, United States authorities picked up the investigation and brought domestic criminal charges based on the foreign government hacking.[48]

These examples are at odds with Ghappour's hypothesis that the use of NITs on the dark web poses a significant threat to international relations. Notably, although Ghappour argues that the use of NITs in this context risks international friction, he points to no examples of it doing so. Ghappour instead draws on instances of foreign opposition in extraterritorial investigations that did not involve NITs or the dark web.[49] We think the better way to gauge the risks of using NITs to light the dark web is to focus on existing practice. In that context, the evidence suggests a norm of cooperation instead of confrontation.[50]

---

44. *See generally* POLICY DEP'T FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, EUROPEAN PARLIAMENT DIRECTORATE-GENERAL FOR INTERNAL POLICIES, LEGAL FRAMEWORKS FOR HACKING BY LAW ENFORCEMENT: IDENTIFICATION, EVALUATION AND COMPARISON OF PRACTICES 18-21 (2017), http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (discussing the use of NITs by different governments).

45. *See* Joseph Cox, *The Strange Case of a Hacked Dark Web Child Porn Site Just Got Stranger*, VICE: MOTHERBOARD (Jan. 26, 2017, 12:30 PM), https://motherboard.vice.com/en_us/article/the-strange-case-of-a-hacked-dark-web-child-porn-site-just-got-stranger. The NIT installed in that case sent communications to a server in France, suggesting that authorities in France were in charge of the investigation. *See id.*

46. *See* Joseph Cox, *Australian Authorities Hacked Computers in the US*, VICE: MOTHERBOARD (Aug. 15, 2016, 7:10 AM), https://motherboard.vice.com/en_us/article/australian-authorities-hacked-computers-in-the-us.

47. *See id.*

48. *See id.*

49. *See, e.g.*, Ghappour, *supra* note 5, at 1115 (discussing the 2002 charges brought by the Russian government against FBI agents who used a criminal suspect's username and password to remotely access his account on a Russian server).

50. The cooperation norm in significant part reflects similar criminal laws and enforcement priorities in investigations involving the dark web. According to a 2014 study, over 80% of visits to websites on the dark web were to websites concerning pedophilia. *See* Greenberg, *Dark-Web Visits*, *supra* note 6. The use of NITs to investigate conduct that is not criminal in every jurisdiction where a search occurred would be much more likely to raise foreign opposition.

II. Does Use of NITs to Investigate Dark Web Cases Violate International Law?

Ghappour also suggests that the use of NITs in dark web cases may violate customary international law's prohibition on a state's extraterritorial exercise of law enforcement functions without consent.[51] Notably, Ghappour does not argue that the use of NITs in this context actually *does* violate international law.[52] Rather, he claims that such practice "begins to unravel" the "harmony"[53] between government practice and international law. Ghappour's position is vague, as it isn't clear what it means for a practice to 'begin[] to unravel" existing "harmony." At the same time, we interpret Ghappour's extended discussion of international law as making the case that use of NITs to light the dark web at least poses a serious risk of violating it.[54]

We are skeptical. Although Ghappour cites a few different authorities on this point, he particularly stresses the rule, articulated by the American Law Institute in a 1987 Restatement, that "[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."[55] That rule, however, is not unqualified. States may take certain judicial or nonjudicial measures, including enforcement measures, against a person located outside their territory.[56] Arguably the type of law enforcement proscribed by the rule is the physical sending of law enforcement officers into the territory of the other state to arrest an offender or to engage in a criminal investigation, not the type of electronic investigation at issue with respect to a Tor case, which involves no physical entry into the state of that kind.[57] All the examples provided in the reporters' notes to the rule involve physical entry by the law enforcement officials of one state into the territory of another state, notably situations of abduction.[58]

Even if the rule covers more than physical entry by law enforcement officers into the territory of another state, the 1987 rule was articulated prior

51. Ghappour, *supra* note 5, at 1117-18.

52. *See id.* at 1108 (concluding that "[i]t is not clear whether (and to what extent) a particular network investigate technique runs afoul of international law or how targeted states may respond").

53. *Id.* at 1106.

54. *See id.* at 1105-08, 1116-18.

55. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (AM. LAW INST. 1987); *see also* Ghappour, *supra* note 5, at 1100-01, 1100 n.127.

56. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 431.

57. *Id.* § 432 cmt. b ("[W]hile a state may take certain measures of nonjudicial enforcement against a person in another state . . . its law enforcement officers cannot arrest him in another state, and can engage in criminal investigation in that state only with that state's consent.").

58. *Id.* § 432 reporters' notes 1-3.

to the rise of the internet, so the question is how such a rule might apply today.[59] As noted above, law enforcement officials around the world engage in various types of "investigation," whether in the form of transnational telephone calls or searching internet sites hosted abroad, that do not involve specific consent by a foreign government. Ghappour himself does not seem to follow the 1987 rule literally; although the rule proscribes a state's law enforcement officers from exercising "their functions in the territory of another state,"[60] Ghappour opines that U.S. criminal investigators can collect "digital evidence located anywhere in the world" so long as they do not use "enforcement mechanisms."[61]

New distinctions are being drawn in the digital age. But what should they be? When it comes to customary international law, the key is understanding the exact contours of contemporary state practice. Like the common law, customary international law is a dynamic source of international law that changes over time; it shapes itself to the contemporary needs of states. When a widespread practice by states exists, either in the form of active practice or in the form of acquiescence to the practice of others, undertaken in a belief that the practice is lawful (referred to as *opinio juris*), then a rule forms around that practice.[62] As such, even on a conceptual level, Ghappour's concern with "harmony" between international law and government practice misconstrues the nature of customary international law, which does not stand alone from government practice but, rather, arises from it.

---

59. In fact, the American Law Institute is now updating its 1987 Restatement. The analogous provision in the latest draft reads: "Under customary international law . . . [a] state may not exercise jurisdiction to enforce in the territory of another state without the consent of the other state." *See* American Law Institute, Restatement of the Law Fourth, The Foreign Relations Law of the United States, Jurisdiction, Tentative Draft No. 3, at 58 (Mar. 10, 2017) (on file with author). Comment a to this section provides: "Jurisdiction to enforce concerns the authority of a state to exercise its power to compel compliance with law." *Id.* Reporters' Note 1 defines "jurisdiction to enforce" as follows:

> Enforcement jurisdiction includes compelling compliance with law through the use of force, as well as the performance of governmental functions whether or not those functions involve the use of force. Examples include arresting a person, detaining a person, serving compulsory process, conducting police or administrative investigations, taking depositions and witness statements, executing an order for the production of documents, seizing property, and enforcing judgments.

Id. at 59. While the new version is still not addressing the issue of the internet or of NITs, the current draft (especially through its examples) continues to suggest physical presence in another state's territory. *See id.* at 59-61.

60. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2).

61. Ghappour, *supra* note 5, at 1101.

62. *See* Int'l Law Comm'n, Rep. on the Work of Its Sixty-Eighth Session, U.N. Doc. A/71/10, at 76 (2016) (listing draft conclusions on the identification of customary international law).

In this particular context, it is doubtful that the rule expressed in the 1987 Restatement is viewed by states today as extending to the use of NITs. First, the 1987 rule is focused on conduct that occurs *exclusively* in a foreign state.[63] Yet use of an NIT is not necessarily such conduct. Depending on the case, the use of an NIT may result in conduct solely within the territory of the state employing it. As a result, application of the 1987 rule in the manner suggested by Ghappour may result in a state being prohibited from using an NIT even to pursue criminal conduct in its own territory. The 1987 rule had (and was intended to have) no such effect.

Second, the premise of the 1987 rule is that it is possible to first obtain consent from the foreign government before acting.[64] In dark web cases, however, the user has taken technological steps to ensure that such consent cannot be obtained by masking the territorial origin of the wrongful conduct. Indeed, a government ordinarily uses an NIT in a Tor case to find out where the user is located so as then to obtain consent from the foreign government for further action. If the 1987 rule applies when Tor is used to hide a location, we might end up in the paradoxical situation in which all nations would want an NIT to be used to reveal those committing a crime and yet no nation would do so because they could not first obtain consent.

The more plausible interpretation of contemporary state practice and *opinio juris*, in light of the cooperation previously discussed, is that states accept the use of an NIT if necessary in a given situation to determine which state's consent is required for further investigative and enforcement purposes. Government use of NITs raises significant policy difficulties. We doubt, however, that such methods force governments into the quandary of either leaving global criminal cases uninvestigated or violating international law.

III. Does Use of NITs Implicate a "Regulatory Vacuum" that Leaves Decisions to "Rank-and-File" Agents?

Ghappour argues that the risks of using NITs are particularly troubling because they occur in a "regulatory vacuum," in which the choice to use NITs is

63. As indicated in the above quoted text, § 432(2) of the 1987 Restatement reads: "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." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (emphasis added). By contrast, § 432(1), which addresses enforcement by a state within its own territory, contains no such requirement of consent by another state. *Id.* § 432(1).

64. The recently-released *Tallinn Manual 2.0*, a careful analysis of how international law applies to cyberspace conducted by nineteen experts from around the world, found "that international law does not address" this type of "situation with clarity." TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 68 (Michael N. Schmitt ed., 2d ed. 2017).

left to the discretion of "rank-and-file" agents.[65] Again, we are skeptical. In our view, Ghappour overlooks two sources of oversight. The first involves the judicial branch, and the second involves the executive branch.

The first source of oversight is the judiciary. Because the government does not know the target computer's location, investigators must obtain a warrant just in case the computer ends up being inside the United States. Ghappour calls this "a bizarre structural arrangement,"[66] apparently because the required warrant doesn't actually authorize the search if the computer turns out to be abroad. But the point remains that the government will have obtained a warrant. The use of the NIT will be reviewed for particularity and probable cause by a federal judge just like in a purely domestic search case.

Ghappour's description of a "regulatory vacuum" also ignores the likelihood of self-imposed executive branch oversight. Ghappour treats the absence of statutory regulation as evidence that "rank-and-file" agents decide when and how to use NITs. This seems unlikely. Law enforcement has every incentive to subject decisions to use NITs to extensive oversight within the executive branch. NITs are very expensive to develop and require a great deal of technical sophistication to use. Drafting an NIT warrant requires considerable legal sophistication and the evaluation of significant legal ambiguities. NIT investigations typically involve international cooperation and coordination. Finally, use of NITs may lead to disclosure of their details in subsequent litigation, potentially depriving the government of future access to computers by using that same vulnerability.[67]

FBI testimony about the Playpen warrant appears to confirm our suspicion.[68] According to an FBI agent involved in the investigation, "several . . . levels of management from both" the FBI and DOJ participated in the deliberations about use of the Playpen NIT.[69] Several sections of Main Justice in Washington, D.C., were involved with the decision,[70] and the FBI Office of General Counsel was also aware of the operation.[71] We suspect this is the norm. If so, something resembling the review Ghappour proposes is already standard practice. Perhaps a statute or other framework would be an improvement. But we are skeptical that Ghappour's description of "rank-and-file" agents acting without oversight is accurate.

---

65. Ghappour, *supra* note 5, at 1106.

66. *See id.*

67. *See, e.g.*, Joseph Cox, *Judge Rules FBI Must Reveal Malware It Used to Hack Over 1,000 Computers*, VICE: MOTHERBOARD (Feb. 18, 2016, 2:20 PM), https://motherboard.vice.com/ en_us/article/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud.

68. *See* Transcript of Motion Hearing at 43-46, United States v. Anzalone, 221 F. Supp. 3d 189 (D. Mass. 2016) (No. 15-10347-PBS).

69. *Id.* at 45 (testimony of Special Agent Daniel Alfin).

70. *Id.* at 44.

71. *Id.* at 46.