2017

Tallinn, Hacking, and Customary International Law

Ahmed Ghappour

doi:10.1017/aju.2017.59

SYMPOSIUM ON SOVEREIGNTY, CYBERSPACE, AND TALLINN MANUAL 2.0

TALLINN, HACKING, AND CUSTOMARY INTERNATIONAL LAW

*Ahmed Ghappour**

Tallinn 2.0 grapples with the application of general international law principles through various hypothetical fact patterns addressed by its experts. In doing so, its commentary sections provide a nonbinding framework for thinking about sovereignty, raising important considerations for states as they begin to articulate norms to resolve the question of precisely what kinds of nonconsensual cyber activities violate well-established international laws—a question that will likely be the focus of international lawyers in this area for some time to come.

This essay focuses on one area of state practice where states are already dealing with these issues: the use of hacking techniques by law enforcement agencies to collect evidence stored on foreign-located computers whose location is *unknown* at the time of the search. It shows how the resulting cross-border cyber-exfiltration operations are in tension with international legal norms, and face a greater risk of public exposure than those conducted by military or intelligence agencies. It then argues that, for the United States, these potential drawbacks may present an opportunity, by providing a specific context for the articulation of norms in cyberspace.

Use of Hacking Techniques

Law enforcement agencies across the globe are adopting hacking techniques to track down criminals who use anonymization tools to hide their location online. In the United States, a modification to Rule 41 of the Federal Rules of Criminal Procedure passed in December 2016, enabling magistrate judges to issue hacking warrants for computers whose location is unknown at the time of the search. In Europe, the United Kingdom, France, and Poland have followed Germany in enacting government hacking statutes. The Netherlands and Italy will likely follow suit this year with statutes of their own.

Hacking techniques are useful for law enforcement in tracking down criminals who have anonymized their communications by using cryptographic software to conduct online transactions without revealing their location to third parties. Without a physical location to search, investigators using conventional investigation methods are left without an evidentiary link between crimes that have occurred in virtual space and a person or computer in the physical world. Hacking techniques enable agents to use the internet to facilitate access and extract information from targeted devices, something that formerly required investigators to operate in the physical world. Once installed, malware can enable investigators to conduct surveillance by collecting files on the targeted device, gathering real-time information, or undertaking any other task the computer can perform.

The nature of the underlying technologies, however, raises questions as to where the relevant police action takes place. As one U.S. Department of Justice official put it, computers targeted by such cyber operations "could be

* *Associate Professor of Law, Boston University School of Law.* *Portions of this essay are drawn from Ahmed Ghappour,* Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075 (2017).*

down the street or on the other side of the planet."[1] Without knowledge of a target's location *before* the deployment of a cyber-exfiltration operation, there is no way to obtain consent from a host country until *after* its sovereignty has been potentially encroached.[2] The resulting cross-border law enforcement operations are a significant deviation from existing state practice. This raises questions as to the legality of such operations and demonstrates the difficulty of applying general principles of law to cyber activities.

Tensions with International Legal Norms

Consider first the principle of state sovereignty, which broadly tells us what states can do and how impacted states may respond. Rule 4 of *Tallinn 2.0* characterizes sovereignty as a primary norm,[3] rather than a foundational principle that underpins primary norms such as the duty of nonintervention.[4] That is, *Tallinn* indicates that sovereignty is a norm from which no derogation is permitted, raising the stakes for violation and the importance of understanding when a violation has occurred. Yet the principle is not defined in any primary international law source, and it is thus difficult to pin down a definition that is acceptable to all.

The *Tallinn* experts were in unison that the physical presence of a state actor in another state's territory was not necessary for a violation of sovereignty to occur. Instead, they assessed whether a sovereignty violation existed based on (1) the degree of infringement on the state's territorial integrity, and (2) whether the cyber operation resulted in a usurpation of "inherently government functions."[5]

As to the first basis, the experts agreed that loss of functionality of a computer could alone constitute a violation of sovereignty, but "no consensus could be achieved as to the precise threshold at which this is so due to lack of expressions of *opinio juris*," cautioning "that state practice based on a sense of legal obligations" was necessary to better clarify whether a given cyber operation violated the norm. At least some experts believed that mere implantation of malware on a computer would suffice to violate another state's sovereignty.

Under the second basis, the experts agreed that if a state's law enforcement actors hack a computer located in another state to obtain evidence for criminal prosecution without first obtaining that state's consent, "the former has violated the latter's sovereignty because the operation usurps an inherently governmental function [law enforcement] exclusively reserved to the territorial State under international law."

This may also constitute a violation of the duty of nonintervention, which, according to *Tallinn*, "prohibits coercive intervention, including by cyber means, by one State into the internal or external affairs of another."[6] While law enforcement is clearly within a state's *domaine réservé*, it is unclear exactly what makes a cyber operation that usurps that domain "coercive." *Tallinn* is clear that a "use of force" is not a requirement for an act to be coercive,

[1] Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post (Dec. 6, 2013) (quote attributed to Jason M. Weinstein, former Deputy Assistant Attorney General in the DOJ Criminal Division).

[2] Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, Just Security (Sept. 14, 2014, 9:10 AM).

[3] This appears to match the State Department's view as promulgated by then-Legal Adviser Brian Egan in 2016. Brian Egan (Legal Adviser, U.S. Dep't of State), Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016). However, it also appears to conflict with the Department of Defense's articulation of sovereignty as a foundational principle underpinning the duties of nonintervention and neutrality in relation to nonhostile states. *See* U.S. Dep't of Defense, Department of Defense Law of War Manual sec. 15.2.1.3, at 951 (rev. Dec. 2016).

[4] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 17 (Michael N. Schmitt gen. ed., 2017) [hereinafter Tallinn 2.0]; *see also* Michael S. Schmitt, *Transparency and International Law in Cyberspace*, Just Security (Nov. 15, 2016, 9:11 AM).

[5] Tallinn 2.0, *supra* note 4, at 20–22.

[6] *Id.* at 312.

but it remains to be understood whether the analysis turns on the acting state's intent, the targeted state's lack of choice, or both.

Law enforcement hacking also raises new jurisdictional difficulties. On the one hand, the *Tallinn* experts agreed that "a State's law enforcement authorities may not hack into servers in another State to extract evidence or introduce so-called white worms to disinfect bots there that are being used for criminal purposes without the territorial State's agreement."[7] Doing so would be an impermissible exercise of enforcement jurisdiction, unless international law provides a specific allocation of authority or the targeted state consents.

On the other hand, international law does not address cases where it is impossible or difficult to determine where the computer subject to enforcement jurisdiction is located. Considering this ambiguity, the *Tallinn* experts were unable to achieve consensus as to whether, and to what extent, a state might be permitted to exercise enforcement jurisdiction in such instances. The *Tallinn* experts did not address the related question of whether the state has a due diligence obligation to take the technologically trivial step of determining the location of the target early on in a hacking operation.[8] This would enable the state to determine whether the target is located overseas, and to cease the mission if that is the case. Nor does *Tallinn* address whether a state must notify the target state, or what effect (if any) such notice would have on the legality of the operation.

Risks and Opportunities

As I have argued before, these doctrinal uncertainties give rise to foreign relations risk.[9] They demonstrate, for example, that it is entirely plausible that a targeted state could characterize another state's cyber-exfiltration operations as a violation of sovereignty, even if the target device's location was unknown when the operation was deployed. Indeed, a recently released report commissioned by the European Parliament concludes that hacking a foreign-located computer that has an unknown location *is* a violation of sovereignty, adding that "[g]iven the scale of these risks, significant debate would be expected at international and EU fora on the use of hacking by national-level law enforcement agencies."[10]

Tallinn itself seems to acknowledge these risks, warning that "the extension of jurisdiction to persons and activities that do not have a substantial connection with the State purporting to exercise such jurisdiction, or that unnecessarily infringes upon another State's sovereignty or upon foreign nationals not located on the first State's territory, can not only lead to international tension, but in some cases constitute an internationally wrongful act."[11] An injured state that characterizes these violations as internationally wrongful acts may turn to self-help measures, which, in turn, risk conflict escalation.[12]

[7] *Id.* at 68.

[8] This due diligence requirement would be satisfied in operations where the sole purpose is to determine a device's location. However, some law enforcement hacking operations are more complicated, seeking more information or intending to otherwise affect the target machine.

[9] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1116–1122 (2017).

[10] Directorate Gen. for Internal Policies, Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices 28 (2017) [hereinafter EU Report] ("This 'loss of knowledge of location' means that, when conducting investigations using hacking techniques, law enforcement agencies risk extraterritorial hacking and breaching the international legal principle of sovereignty." (citations omitted)).

[11] Tallinn 2.0, *supra* note 4, at 61.

[12] Ghappour, *supra* note 9, at 1116–1122.

In this way, *Tallinn* joins the chorus of scholars and policymakers calling for clear guidelines and transparent norms in cyberspace, warning of potentially harmful consequences for international relations if the status quo is maintained.[13]

Yet the surreptitious nature of cyber activities means that states have not been put in the position where they have had to defend their actions or omissions in cyberspace based on international law. It is very difficult to attribute a sophisticated cyber operation to the responsible state or entity: the evidence is typically circumstantial,[14] highly technical,[15] and often derived from intelligence sources and methods that governments keep secret.[16] While international law does not set out an explicit burden or standard of proof to meet when one state attributes an act to another state, the uncertainties inherent in attribution may generate doubt about the legitimacy of any response taken on its basis, especially when faced with denial by the accused country.[17]

This dynamic has allowed cyber-sophisticated states to enjoy a certain amount of operational and strategic flexibility in the scope of cyber activities undertaken by their military and intelligence actors. States facing attribution difficulties may hesitate to initiate protest or self-help for fear their response will not be perceived as legitimate in the international community. Accused states may feel less pressure to defend their alleged actions or omissions based on international law. And institutions and policymakers may be less inclined to spend resources promulgating norms that cannot be enforced for lack of attribution.

By contrast, law enforcement cyber-exfiltration operations may be subject to a greater risk of public exposure than those conducted by military or intelligence agencies. For example, procedural safeguards in the American criminal justice system provide many opportunities for public disclosure of direct evidence linking law enforcement actors to a particular incident. This may include testimony by the agent that launched the cyber-exfiltration operation, disclosure of its malware components, or information about the computers that were infected.[18] As a result, attribution of cross-border network investigative techniques (i.e., law enforcement hacking) to the United States is more likely to be based on direct evidence that stands on its own and that is already in the public domain.[19]

It is thus in the United States' interest to take a leadership role in clarifying and developing existing norms as applied to cross-border law enforcement hacking. Without the articulation of specific norms on when, how, and who law enforcement actors should be permitted to hack, cross-border cyber operations that are attributed to U.S. law enforcement may send unintended signals to other states. For example, U.S. law enforcement has primarily used hacking techniques to investigate bomb threats and child pornography, but the Department of Justice has been explicit in its intent to use the new investigatory technique without limit to the crime being investigated.[20] For

[13] This view was recently endorsed by the Obama State Department's Brian Egan in remarks at Berkeley, Egan, *supra* note 3; and in a report commissioned by the European Parliament, EU Report, *supra* note 10, at 28. *See also* Ghappour, *supra* note 9, at 1108–1122.

[14] *See, e.g.*, Ghappour, *supra* note 9, at 1109.

[15] *See, e.g.*, Herbert Lin, *Attribution of Malicious Cyber Incidents* 13–15 (Hoover Working Group on National Security, Technology, and Law, Aegis Paper Series No. 1607, 2016).

[16] *Id.* at 14.

[17] *See* Egan, *supra* note 3.

[18] For example, in a recent case the government was ordered to disclose information about thousands of computers it hacked that were in over a hundred foreign countries. Transcript of Evidentiary Hearing at 39:15–23, United States v. Tippens, No. 16-cr-5110-RJB (W.D. Wa. Nov. 1, 2016).

[19] Making matters worse, once a foreign nation attributes a specific incident to a source, the attack's technical characteristics can be used to attribute (and defend against) other, potentially more malicious, cyber attacks from the same source.

[20] *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, Advisory Comm. on Rules of Criminal Procedure: April 2014, at 179 (2014).

example, the technique was recently used in a cyber stalking investigation.[21] The targeted computer was located in the United States, but could have just as easily been anywhere in the world. Does this signal that Russian law enforcement investigators are entitled to hack U.S.-located computers so long as they are investigating a violation of *any* Russian criminal law? More recently, the German parliament passed legislation authorizing its law enforcement agencies to use hacking techniques in a wider range of criminal investigations, including drug trafficking, bribery, and sex crimes.[22]

Questions about precisely what kinds of cyber activities violate state sovereignty, the principle of nonintervention, and the prohibitions on the exercise of enforcement jurisdiction will be the subject of debate for some time to come. States inclined to resolve conflicts and minimize significant uncertainties may promulgate international cyberspace norms applicable to law enforcement to set a baseline on activities and build trust amongst stakeholders. In international law, gaps in the *lex lata* must be filled not by academics but by states, whether through universal agreement, a patchwork of bilateral or multilateral agreements, or by state practice and *opinio juris*.

Conclusion

The state practice of law enforcement hacking presents an opportunity for the United States and its allies to promulgate their positions on enforcement jurisdiction norms in cyberspace in a manner that allows cross-border hacking in limited situations, while preventing unnecessary violations of sovereignty. There is historic momentum in law enforcement cooperation between states, and there is an interest in drawing clearly delineated norms for instances in which the target location is unknown at the time of deployment. This is particularly the case given the lower barriers of entry for unsophisticated states that wish to use remote access tools to gather evidence from potentially foreign-located computers to solve crimes.[23]

Specific areas where the interests likely converge include (a) setting a range of crimes that may trigger the use of hacking techniques, (b) delineating the breadth of hacking techniques that may be deployed against targets whose location is unknown, and (c) requiring a showing of culpability of the individuals whose property interests are impacted in such operations. As I have argued before, law enforcement hacking operations should be limited to instances where (a) the investigation pertains to especially heinous crimes, such as terrorism, child pornography, human trafficking, and international organized crime; (b) the malware used is programmed to cease operation once it determines it has breached an overseas target; and (c) the investigators are able to make a reasonable showing that the property interests impacted are those of a criminal actor.

[21] Thomas Fox-Brewster, *That Time the FBI Phished a Cop with Poisoned Microsoft Docs*, Forbes (May 30, 2017, 3:55 PM).

[22] Joseph Cox, *Germany Just Gave Cops More Hacking Powers to Get Around Encryption*, Motherboard (June 22, 2012, 1:12 PM).

[23] The lower barriers of entry exist at least in part because targeting civilians is far easier than targeting protected government systems or corporations that have resources to mount cyber defenses.