doi:10.1017/aju.2017.5

SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

THE U.S. ELECTION HACKS, CYBERSECURITY, AND INTERNATIONAL LAW

*David P. Fidler**

Introduction

In October 2016, the United States accused Russia of hacking political organizations involved in the U.S. elections and leaking pilfered information to influence the outcome.[1] In December, President Obama imposed sanctions for the hacking.[2] This incident damaged President Obama's cybersecurity legacy. The "hack and leak" campaign targeted American self-government—a challenge to his administration's promotion of democracy in cyberspace. It created problems for the president's emphasis on international law and norms as "rules of the road" for cybersecurity. The episode exposed failures in his attempts to make deterrence an important instrument of U.S. cybersecurity.

The election hacks mean democracy promotion, international law and norms, and deterrence face grim prospects in cybersecurity.[3] However, this reality might not matter to President Trump, who shows little interest in prioritizing democratic values or international law and norms in cybersecurity policy. President-elect Trump's disparagement of the intelligence community's conclusions about Russian involvement in the hacks, grudging acceptance of these findings, and desire to improve relations with Russia mean this incident will not inform his approach to deterrence in cybersecurity. Thus, this disturbing episode is unlikely to have much impact on the new administration's cybersecurity policies.

The Election Hacks in Cybersecurity Context

The Obama administration's handling of the "hack and leak" operation reflects patterns exhibited in other incidents where it accused foreign governments of malicious cyberactivities against the United States. The administration indicted Chinese military personnel for economic cyberespionage against American corporations.[4]

* *James Louis Calamaras Professor of Law, Indiana University Maurer School of Law and Adjunct Senior Fellow for Cybersecurity, Council on Foreign Relations.*

[1] Director of National Intelligence, Press Release, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security (Oct. 7, 2016).

[2] White House, Executive Order-Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities (Dec. 29, 2016).

[3] Adam Segal, *Do U.S. Efforts to Deter Russian Cyberattacks Signal the End of Cyber Norms?*, NET POL. (Nov. 7, 2016).

[4] Department of Justice, Press Release, U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage, (May 17, 2014).

North Korea was held responsible for hacking Sony in an attempt to prevent a film's release.[5] The U.S. government filed criminal charges against Iranian personnel for distributed denial of service attacks against financial institutions and unauthorized access to computers at a dam in New York.[6]

The Chinese, North Korean, and Iranian incidents did not involve illegal uses of force or armed attacks. Whether these incidents violated the principles of sovereignty and nonintervention was analyzed under the international law on countermeasures.[7] However, as the Obama administration progressed, frustration with international law and norms grew as cyberthreats mounted seemingly unabated. This frustration produced increasing interest in deterrence by punishment as a way to strengthen U.S. cybersecurity.

The Obama administration pursued different kinds of deterrence for cybersecurity. Its emphasis on cyberdefenses sought deterrence by denial—denying adversaries benefits they seek through cyberoperations.[8] Efforts to clarify international law and develop cybernorms aimed to generate deterrence by norms.[9] The administration also included deterrence by punishment. It warned it would "ensure that the risks associated with attacking or exploiting our networks vastly outweigh the potential benefits"[10] and convince adversaries they "will suffer unacceptable costs" if they harm the United States through cybermeans.[11]

Each type of deterrence implicates international law differently. Deterrence by norms uses international law to deter malicious cyberactivities. Deterrence by denial involves defensive actions that raise few concerns under international law. Deterrence by punishment functions through threats or infliction of disproportionate costs on adversaries for harming U.S. interests. This logic diverges from international law on countermeasures, which requires proportionate responses and prohibits punishing the state responsible for internationally wrongful acts.

During the Obama administration, deterrence by punishment gained more attention because deterrence by denial and deterrence by norms were not proving effective. The election hacks reinforced this perception. Despite years of government emphasis on the need for strong private-sector cyberdefenses, the Democratic National Committee failed to implement even basic cybersecurity measures.[12] The Russian attempt to influence the elections challenged the effectiveness of international law and norms. The election hacks produced calls for President Obama to punish the Kremlin to deter Russia and other countries from engaging in such behavior in the future.

The Obama Administration, International Law, and Cybernorms

This state of affairs is not what President Obama sought when he made cybersecurity a priority and stressed the importance of international law and norms in this area. The *International Strategy for Cyberspace* claimed the internet's growth has "not been matched by clearly agreed-upon norms for acceptable state behavior in cyberspace."[13] The

[5] David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea after Sony Case*, N.Y. Times (Jan. 3, 2015).

[6] Department of Justice, Press Release, Manhattan U.S. Attorney Announces Charges against Seven Iranians for Conducting Coordinated Campaign of Cyber Attacks against U.S. Financial Sector on Behalf of Islamic Revolutionary Guard Corps-Sponsored Entities (Mar. 24, 2016).

[7] *See, e.g.,* Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, Just Security (Dec. 17, 2014); Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, UN Doc. A/56/10 (2001).

[8] Annegret Bendiek & Tobias Metzger, *Deterrence Theory in the Cyber-Century* 6-7 (May 2015).

[9] Tim Stevens, *A Cyberwar of Ideas? Deterrence and Norms in Cyberspace*, 33 Contemp. Security Pol'y 148, 159 (2012).

[10] White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 13 (May 2011).

[11] Department of Defense, Cyber Strategy 11 (Apr. 2015).

[12] Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. Times (Dec. 14, 2016).

[13] White House, *supra* note 10, at 9.

https://doi.org/10.1017/aju.2017.5 Published online by Cambridge University Press

administration wanted to clarify how international law applied in cyberspace and develop norms for "peaceful and just interstate conduct" in cyberspace.[14]

This pursuit of norms and international legal clarity emerged in contentious circumstances. The administration inherited rifts over internet governance. Since the late 1990s, China and Russia have promoted intergovernmental control over internet governance instead of the multi-stakeholder approach the United States supports. China and Russia favor using international law in internet governance, but the United States rejects this idea.

This fault line converged with other problems. The Chinese and Russian positions on internet governance stressed the primacy of sovereignty. "Internet sovereignty" captured how these and other countries defined security in cyberspace to include cyberattacks, political activities on the internet, and the content of online communications. China, Russia, and like-minded nations articulated norms reflecting internet sovereignty.[15]

The United States championed "internet freedom." Secretary of State Hillary Clinton declared everyone had the right to connect to an open, global internet and enjoy freedom of expression online. To promote this right, the U.S. government supported efforts "in more than 40 countries to help individuals silenced by oppressive governments" by empowering people to engage in free expression, circumvent censorship, and access the internet.[16]

Disclosure of the Stuxnet attack on Iran[17] and Edward Snowden's revelations[18] damaged the Obama administration's strategy of developing cyber "rules of the road" within the framework of internet freedom. For many, the Stuxnet operation violated international legal obligations on sovereignty, nonintervention, and nonuse of force. Snowden sparked controversies about U.S. offensive cyberoperations, surveillance, and espionage. Whether U.S. surveillance violated human rights law proved particularly contentious.

Despite Stuxnet and Snowden, the Obama administration claimed progress on international law and norms. The United States worked to increase accession to the Budapest Convention on Cybercrime, and the number of parties grew between 2009 and 2016.[19] However, participation remained limited, and states in other regions developed different treaties. Cybercrime grew globally after President Obama took office, demonstrating the various treaties do not deter cybercrime.

The Obama administration believed it advanced international law and norms in the UN Group of Governmental Experts (GGE) tasked to consider cybertechnologies and international security.[20] In 2013, the GGE reached consensus that international law applies in cyberspace.[21] In 2015, it offered nonbinding norms for UN members to consider, including two the United States promoted:

- States should not conduct or support cyberoperations that damage or impair critical infrastructure or harm information systems used by another state's computer emergency response teams; and

[14] *Id.*

[15] International Code of Conduct for Information Security, UN Doc. A/69/723 (Jan. 23, 2015).

[16] Secretary of State Hillary Clinton, Remarks on Internet Freedom (Jan. 21, 2010).

[17] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012).

[18] Free Snowden.

[19] Council of Europe Convention on Cybercrime, Nov. 23, 2001, E.T.S. 185.

[20] *Developments in the field of information and telecommunications in the context of international security*, United Nations Office for Disarmament Affairs.

[21] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 8, UN Doc. A/68/98* (June 24, 2013).

https://doi.org/10.1017/aju.2017.5 Published online by Cambridge University Press

- States should respond to requests for assistance by other states whose critical infrastructure experiences malicious cyberacts.[22]

However, these actions did not represent progress. The 2013 report appeared as Snowden's disclosures generated accusations that U.S. cyberactivities violated international law. Chinese economic cyberespionage, Iranian hacking of a New York dam, North Korea's operations against Sony, and Russia's "hack and leak" campaign continued or occurred after the GGE agreed international law applied in cyberspace.

Some norms in the 2015 report simply restated international law. The principles of sovereignty, nonintervention, and nonuse of force already proscribe damaging critical infrastructure in another state. The norm that a state should not allow its territory to be used for internationally wrongful cyberacts mirrors the international legal rule that states cannot permit their territories to be used to cause harm in other states. The norm that states should respond to requests for assistance from other states experiencing malicious cyberactivities does require assistance be provided. Other norms are mere exhortations (e.g., protect critical infrastructure).

The Obama administration wanted international law and cybernorms to support internet freedom. However, Freedom House concluded in 2016 that internet freedom had declined for six consecutive years.[23] The GGE's statement in 2013 that international law, which includes human rights law, applied in cyberspace and the 2015 GGE report's norm on respecting human rights online have had no discernable impact on internet freedom.

The United States achieved a breakthrough with China in 2015 when both governments agreed not to engage in economic cyberespionage.[24] This norm then appeared in agreements between China and the United Kingdom and China and Germany. The Group of 20—including Russia—also accepted it.[25] Previously, the United States had failed to get other countries to renounce economic espionage, and international law continued not to regulate this type of espionage.

Why a norm against economic cyberespionage achieved global acceptance is not clear. However, the story involves U.S. indictments of Chinese military personnel and threats to sanction Chinese companies benefiting from economic cyberespionage against American enterprises—deterrence by threats of punishment for harming U.S. interests.[26] The Obama administration also turned to deterrence by punishment in responding to malicious cyberoperations attributed to North Korea and Iran.

Deterrence by Punishment in Cybersecurity: Policy and International Legal Implications

By the elections hacks, deterrence by punishment had become more important to U.S. cybersecurity than previously was the case. The Obama administration's resort to sanctions in response to Russian cybermeddling reinforced this prominence. This trajectory intensified debates about deterrence as a cybersecurity strategy. Experts disagreed whether deterrence concepts—including the need for clear attribution, credible retaliatory threats and actions, and escalation dominance—made sense in the cyberrealm. The sanctions against Russia agitated these disagreements and raised questions about how international law and norms connected with deterrence strategy.

Given the prominence of deterrence by punishment, the Obama administration's response to the election hacking became a seminal event. However, the response did not end debates about deterrence by punishment in

[22] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at 8, UN Doc. A/70/174 (July 22, 2015).

[23] Freedom House, *Freedom on the Net 2016* (Nov. 2016).

[24] White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015).

[25] *About G20*, G20.

[26] Ellen Nakashima, *U.S. Developing Sanctions against China over Cyberthefts*, Wash. Post (Aug. 30, 2015).

https://doi.org/10.1017/aju.2017.5 Published online by Cambridge University Press

cybersecurity. Attributing the hacks to Russia triggered attacks by candidate and President-elect Trump on the intelligence community, a spectacle ending with Trump's truculent acknowledgement of Russian involvement. For many experts, the information the Obama administration provided on Russian culpability was underwhelming,[27] which added to the attribution controversy.

The sanctions sparked arguments about whether they were sufficient to deter Russia or other countries from cybermeddling in future elections. President-elect Trump's hostility towards the intelligence community and interest in better relations with Russia undermined the sanctions' credibility as a deterrent. Doubts about the deterrent effect of President Obama's threat of covert cyberoperations against Russia increased when the Director of National Intelligence argued the United States "cannot put a lot of stock ... in cyber deterrence."[28] Nor did the sanctions clarify matters concerning escalation dominance. Russia decided not to retaliate, brushing off the sanctions as insignificant in anticipation of Trump taking office.

The Obama administration's response also produced scrutiny concerning its emphasis on international law and norms in cybersecurity. President Obama stated the actions were "a necessary and appropriate response to efforts to harm U.S. interests in violation of established norms of behavior."[29] His administration consistently distinguished norms from international law, meaning it concluded the election hacking did not violate international law.

This choice constitutes important state practice on when cyberactivities transgress the principles of sovereignty and nonintervention. However, it means international law creates no deterrence by norms against similar cybermeddling in future elections in democratic countries. Coming from an administration that sought to strengthen international law's role in cybersecurity and promote democracy in cyberspace, this outcome undermines the pursuit of cyber-"rules of the road" and harms internet freedom.

The Obama administration's claim Russia violated an established norm reveals failures concerning deterrence by norms and cybernorm development. First, the claimed norm did not deter Russia from conducting malicious cyberoperations against democracy in the United States. Such interference suggests the established norm carried no significance for Moscow.

Second, whether the election hacks violated an accepted norm is questionable. When this norm was established is not clear. It does not appear in the Obama administration's efforts in, for example, the GGE. Arguments that President Trump should include a prohibition on using stolen information to influence elections in a new U.S.-Russia cyberagreement indicate this norm was not established.[30] Even domestically, President Obama had to amend an executive order because existing authorities did not address what Russia did.

These doubts connect to President Obama's admission that "developing international norms" for cybersecurity "is in its infancy" because "the most sophisticated state actors—Russia, China, Iran—don't always embody the same values and norms we do."[31] Skepticism about the "established norm" weakened the justification for U.S. retaliation, hurt claims the administration made progress on cybernorms, and damaged internet freedom.

[27] Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (Jan. 6, 2017).

[28] *Transcripts: U.S. Intel Chiefs Testify on Russian Hack*, CNN (Jan. 5, 2017).

[29] White House, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016).

[30] Michael McFaul & Amy Zegart, *America Needs to Play Both the Short and Long Game on Cybersecurity*, WASH. POST (Dec. 19, 2016).

[31] *Barack Obama, Neural Nets, Self-Driving Cars, and the Future of the World*, WIRED (Oct. 12, 2016).

https://doi.org/10.1017/aju.2017.5 Published online by Cambridge University Press

With the Trump administration, the politics of the election hacks will change. As President-elect, Trump made clear he wanted to move past the controversy and strengthen cooperation with Russia. During the campaign, Trump embraced deterrence by punishment in promising to ensure the United States can "launch crippling cyber counter-attacks" as a "deterrent against attacks on our critical resources."[32] His statements as a candidate did not identify internet freedom or international law and norms as important for his plans for cybersecurity.

Given these positions, President Trump is unlikely to implement deterrence by punishment over the election hacks or use this incident to focus on internet freedom or international law and cybernorms. Thus, the election hacks will not produce answers to pressing questions in cybersecurity about deterrence, international law, norms, and democracy promotion.

These questions will not go away. Various bodies have advised the new administration to address deterrence, international law, norms, and internet freedom in its cybersecurity policies. The Center for Strategic and International Studies' Cyber Policy Task Force noted how "the search for an effective deterrent policy … dogged the last two administrations" and advocated improving the "ability to deter attackers by developing a full range of response and countermeasures that go beyond the threat of military action."[33] The President's Commission on Enhancing National Cybersecurity recommended the Trump administration promote "a common understanding of the application of international law in cyberspace" and "develop a strategy for expanding the adoption of cybersecurity norms of behavior in cyberspace during peacetime."[34] New America urged the Trump administration to "strengthen global internet freedom."[35]

Events will force President Trump's hand. Congressional investigations of the election hacking and potential Russian cybermeddling in upcoming European elections might alter President Trump's policies. New malicious cyberactivities against the United States and its allies will require the Trump administration to interpret international law, ponder the utility of norms, deter adversaries, and strengthen democratic solidarity in cyberspace. However, when this reckoning arrives, the opportunity to learn the harsh lessons of the election hacking episode might be lost.

[32] Donald J. Trump Promises Immediate Action on Cybersecurity in His Administration (Oct. 3, 2016).

[33] Center for Strategy and International Studies' Cyber Policy Task Force, A Cybersecurity Agenda for the 45th President (Executive Summary) 1-2 (Jan. 4, 2017).

[34] President's Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy 48 (Dec. 1, 2016).

[35] Rebecca MacKinnon et al., *Internet Freedom at a Crossroads: Recommendations for the 45th President's Internet Freedom Agenda* (Dec. 2016).

https://doi.org/10.1017/aju.2017.5 Published online by Cambridge University Press