CYBERSECURITY, INTERNATIONAL LAW, AND THE FIRST YEAR OF THE TRUMP ADMINISTRATION

*Brian J. Egan**

TEMPLE UNIVERSITY BEASLEY SCHOOL OF LAW – OCTOBER 17, 2017

TABLE OF CONTENTS

I. INTRODUCTION

Thank you to Daniel Cole for that kind introduction, and thanks to Professor Hollis and to the Temple International & Comparative Law Journal for inviting me to speak with you today. I am very happy to be here, particularly at the invitation of Professor Hollis, my fellow alumnus from the U.S. Department of State Office of the Legal Adviser.

I am speaking with you about a topic in which I took a great deal of interest as a U.S. government official, and have continued to follow with interest from the private sector: developments in international law and cyberspace, with a particular focus on the behavior of state actors in cyberspace. I am here to offer some reflections from my own experiences in U.S. government service, and some observations on the state of affairs in cybersecurity and international law in the United States after the first nine months of the Trump Administration.

What I am about to say reflects my personal views alone, and does not reflect the views of the US government or anyone else. After working for over a decade in the US government, I can tell you that it is liberating to speak in a personal capacity on the issues, but you should not take anything I say as official U.S. government doctrine, or even as well-considered or wise! I would welcome your questions and comments at the end of my remarks.

* * *

I want to commend the Journal for the topic of today's symposium, which is "Cyberspace: On the Frontier of International Law, Security, and Diplomacy." I agree that cyberspace is, to some extent, a frontier that raises new questions about appropriate state behavior. And states must consider each of the three dimensions that are the focus of today's symposium—international law, security, and diplomacy—in deciding critical questions about their own behavior in cyberspace.

During my time in the Obama administration, the United States government spent a great deal of time trying to make progress on distilling and articulating the

U.S. position on questions of international law, security, and diplomacy in cyberspace. Progress was demanded by different parts of the U.S. government. U.S. military and intelligence community leaders were concerned about U.S. capabilities; U.S. law enforcement professionals were concerned about state-sponsored criminal activity in cyberspace; and those in the diplomatic community were focused on maintaining U.S. leadership in developing accepted principles for international behavior.

We had interagency meetings and sometimes heated debates with legal and policy officials from every national security-related department and agency. We set forth numerous public pronouncements, including a speech that another former State Department Legal Adviser, Harold Hongju Koh, gave at the National Security Agency in 2012.[1] In Professor Koh's talk in 2012, the United States acknowledged—for the first time, believe it or not—that international law does apply in cyberspace.[2] I gave a follow-up talk at the University of California-Berkeley School of Law in 2016, further articulating the U.S. position on international law and cybersecurity.[3] In the international arena, the United States discussed issues of cyberspace law and policy within the United Nations (U.N.) Group of Governmental Experts (GGE) on information and telecommunications—the United States consulted on cybersecurity with allies and strategic adversaries, and heard from and read what the academy had to say on the topic.

To say that we [in the Obama administration] spent a great deal of time on

---

These—adapted for print— are the remarks prepared by Brian J. Egan for a lecture co-hosted by the Temple International & Comparative Law Journal *and Institute of International Law & Public Policy at Temple University Beasley School of Law on Oct. 17, 2017, and inspired by the development of issue 32.2 of this Journal. The genesis for the essays that comprise issue 32.2 of this Journal was a May 2017 workshop hosted at Temple University, and co-hosted with Leiden University. Under the theme "Influencing International Behavior in Cyberspace: Devising a Playbook of Consequences for Cyber Incidents," the workshop gathered a broad array of academic and governmental experts. Participants included representatives of the Estonian, Finnish, and U.S. governments (including officials from the Department of Defense, the State Department, and the U.S. Trade Representative). All government officials, however, participated in their personal capacity. As such, the views expressed in this special issue should not be attributed to any government or government agency.*

* Partner, Steptoe & Johnson LLP. Former U.S. State Department Legal Adviser (Feb. 22, 2016 – Jan. 20, 2017); Legal Adviser to the National Security Council, Deputy Assistant to the President, and Deputy Counsel to the President (2013–2016); Assistant General Counsel for Enforcement and Intelligence at the U.S. Department of the Treasury (2012–2013); Deputy Legal Adviser to the National Security Staff, Special Assistant to the President, and Associate Counsel to the President (2011–2012); Deputy Legal Adviser to the National Security Staff (2009–2011); Attorney-Adviser at U.S. Department of State (2005–2009); Associate at Goodwin Procter, LLP (fornerly Shea & Gardner) in Washington, D.C. (2000–2005). J.D., U.C. Berkeley School of Law; B.A., Stanford University.

1. Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. ONLINE 1 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

2. *Id.* at 3.

3. Brian J. Egan, Legal Adviser, U.S. Dep't. of State, Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016), *in* Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 169 (2017).

issues related to international law and cyberspace, however, is not meant to suggest that we resolved every issue. As I will discuss further in few minutes, the U.S. position, and the international consensus position, on a number of critical international law questions related to state behavior in cyberspace remains unresolved.

During our time together, I will also provide some observations on how the current administration has addressed issues of international law and cyberspace. In several areas—from the Paris Agreement on climate change to the Iran nuclear deal—the Trump administration has strongly opposed the Obama administration's positions on international law, security, and diplomacy. Despite that, having observed the Trump administration from the outside for its first nine months,[4] I believe that the Trump administration has—perhaps surprisingly—continued to embrace the importance of international law, and the development of international rules, in cyberspace. Below, I will add further detail to that topic while offering a few theories as to why I think that this is the case, in a few minutes. I will also offer some observations on a few of the critical cybersecurity international law questions that remain unanswered.

II. CYBERSPACE: ON THE FRONTIER OF INTERNATIONAL LAW, SECURITY, AND DIPLOMACY

Before we get into some of the current issues facing the U.S. and the Trump administration, let us begin with the basics: Why do all of the issues in this symposium—international law, security, and diplomacy—matter in developing sensible cybersecurity policies?

Let us tackle the most obvious frontier first—security. The need for sound cybersecurity practices and defenses is not an academic or theoretical problem—it is an essential aspect of national security for the U.S. and other countries. Events over the course of the past several months have only confirmed the seriousness of the security aspect of responsible cybersecurity, including protection from state-sponsored cyberattacks.

Take Russia's interference in the U.S. presidential election. The declassified assessment released by the U.S. intelligence community in January 2017[5] includes multiple sobering conclusions on Russian cyber capabilities and U.S. cybersecurity vulnerabilities, including on Russia's cyber espionage against U.S. political organizations and Russian cyber intrusions into state and local election boards.

Or turning to an even more current topic, which is North Korea's apparent advancement of its cyber capabilities: The New York Times[6] and The Wall Street

4. This address was delivered on October 17, 2017, nine months into the Trump administration.

5. *See* OFF. OF THE DIR. OF NAT'L INTELLIGENCE, BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION (2017) ("'Assessing Russian Activities and Intentions in Recent US Elections' is a declassified version of a highly classified assessment that has been provided to the President and to recipients approved by the President.").

6. David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed*

Journal[7] have published fascinating and troubling articles over the last few weeks detailing the recent growth in the intensity and sophistication of North Korea's cyber operations. One former British intelligence official quoted in The New York Times estimates that North Korea's annual take from cyber-enabled theft and ransomware is as high as $1 billion per year.[8] North Korea has also shown a capability to disrupt network operations—remember the Sony Pictures cyberattack from 2014 related to Sony's release of the "The Interview" movie. The Times article closes with what it characterizes as the "big question," which is "whether [Kim Jong-un], fearful that his nuclear program is becoming too large and obvious a target, is focusing instead on how to shut down the United States without lighting off a missile."[9] Thus, it is clear that real security concerns will dominate current U.S. discussions about cybersecurity.

The second frontier, and our focus here, is international law. It is my view that clarification of how international law applies to cyberspace will be critically important to developing an appropriate international framework for state activities in cyberspace. This may be a relatively uncontroversial proposition to most readers of this paper, but many critics question whether it is worth the candle to clarify international law in cyberspace. Some of this criticism reflects a skepticism as to the value of international law in regulating state behavior more generally. "Because international law cannot be enforced, why does it matter?" is one common criticism. A second is that international law is a proxy for a code that allows powerful nations like the United States to operate in a manner of their choosing in the world.

To briefly address the first straw man: Why does it matter whether an activity violates international law? It matters, of course, because the community of nations has committed to abide by international law, including with respect to activities in cyberspace. International law enables states to work together to meet common goals, including the pursuit of stability in cyberspace. And international law sets binding standards of state behavior that not only induce compliance by states but also provide compliant states with a stronger basis for criticizing—and rallying others to respond to—states that violate those standards.

Does this mean that North Korea will abide by international law in cyberspace? Probably not. But this is not a phenomenon that is unique to cyberspace. With respect to international law, Louis Henkin famously said that "It is probably the case that almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time."[10] International law is not perfect and the scope of state compliance is often unclear. Still, in my view, it reflects a remarkable area of international cooperation—an area where states voluntarily agree to bind

---

at North Korean Cyberpower. No More., N.Y. TIMES (Oct. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

7. Timothy W. Martin & Kwanwoo Jun, *'Ridiculous Mistake' Let North Korea Steal Secret U.S. War Plans*, WALL ST. J. (Oct. 11, 2017, 11:34 AM), https://www.wsj.com/articles/north-korea-allegedly-used-antivirus-software-to-steal-defense-secrets-1507736060.

8. Sanger, Kirkpatrick & Perlroth, *supra* note 6.

9. *Id.*

10. COLUM. L. SCH., *The Quotable Louis Henkin*, http://www.law.columbia.edu/louis-henkin/quotable-louis-henkin (last visited Apr. 11, 2018).

themselves to rules that constrain their own behavior in the interests of international peace and stability.

As Professor Koh stated in 2012, "[i]f we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law."[11] Working to clarify how international law applies to states' activities in cyberspace serves those ends, as it does in so many other critical areas of state activity.

As to the second strawman: Is international law simply a proxy that permits the United States and other powerful countries to do as they please, while constraining the behavior of the rest of the world? Based on my own governmental experience, I would submit that the answer is "No." International law is effective because it establishes a set of common ground-rules, and these rules can and do constrain the activity of all countries, including the United States. This has been part of the difficulty for the United States in articulating its positions.

Now, regarding the question of the application of international law to cyberspace, some say that cybersecurity is different and will require perhaps a different approach to international law. Colonel Gary Corn, the Staff Judge Advocate to U.S. Cyber Command, has written that "the uniqueness and rapidly evolving nature of cyberspace will place adaptive pressure on most of the existing international legal framework."[12] I happen to agree with Colonel Corn.

Does this mean, however, that a "new" international law is required to address cybersecurity? In my view, again, the answer is "No." The same international law principles that apply to other state behavior—through treaty or through customary international law—should serve as the baseline for any discussions of the application of international law in cyberspace. International law is not inflexible. It is designed to be adapted through state practice, *opinio juris*, and the development of treaties and other legal instruments to reflect international developments. It is my view that where cybersecurity threats materialize in ways that make it difficult to apply traditional international law principles, states cannot put their heads in the sand—they can and must adapt their thinking in a responsible fashion. More on that in a moment.[13]

Third, diplomacy—like security and international law—is critical to sound cybersecurity policy and practice. At its heart, this means that states must talk to each other about cybersecurity threats and the appropriate rules for cybersecurity. These challenges must be discussed in all areas of government—defense, intelligence, foreign affairs, law enforcement, and homeland security—and by both policy officials and lawyers.

International law goes hand-in-hand with diplomacy. International law is meaningless if states do not talk to and debate with each other about the relevant

11. Koh, *supra* note 1.

12. Gary Corn, *Tallinn Manual 2.0 Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

13. *See infra* Part III.

rules or explain publicly their articulation of the relevant rules. "Diplomacy" does not mean "international harmony and consensus." Disagreements are a core feature of diplomacy. If other countries agreed with U.S. policy without hesitation, I would agree with the Trump administration that the United States would not need such a large State Department, but that is not the world in which we live.

In short, many countries have disagreed with the United States' approach to and interpretations of international law over the years. This is natural and will always be true. But government-to-government dialogue about international law is critical.

Some say that the field of cyberspace and cybersecurity does not lend itself to traditional work on international law in the public sphere because so much state behavior in cyberspace is conducted in secret. It is doubtlessly true that the secret nature of state behavior in cyberspace adds to the challenge of articulating the applicable international legal framework. But this cannot mean that the framework should be developed in secret. In my view, it is risky, and potentially harmful, to the goals of international peace and stability to develop international law in secret. Secret law can lead to misunderstandings between states, or worse.

III. RECENT DEVELOPMENTS IN CYBERSECURITY AND INTERNATIONAL LAW

Next, I would like to take a look at some of the key cybersecurity legal and diplomatic developments over the past nine months. As I mentioned at the outset, in some key respects the Trump administration appears to be following the approach of the Obama administration in advancing an international cyberspace agenda that is based on diplomacy through the development of international law and other rules of the road.

Let us start with the work of the U.N. GGE on Cybersecurity—or Developments in the Field of Information and Communications Technologies in the Context of International Security. The U.N. General Assembly has recognized for nearly twenty years that activities in cyberspace pose potential security threats; its first resolution on this topic was adopted in 1998.[14] The U.N. General Assembly has established five GGEs on this topic to discuss existing and potential threats from the cyber-sphere, and possible cooperative measures that states can consider to address these threats.[15]

Each GGE has consisted of representatives of the permanent members of the U.N. Security Council—China, France, Russia, the United Kingdom, and the United States—as well as a representative group of other member states.[16]

Progress in the GGEs has been incremental and erratic. The first GGE, which was established in 2004,[17] concluded without any substantive agreements. The second GGE was established in 2009 and reached a set of conclusions in

14. Fact Sheet, United Nations Office for Disarmament Affairs, Developments in the Field of Information and Telecommunications in the Context of International Security (Jan. 2014), https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2014/01/Information-Security-Fact-Sheet-Jan-2014.pdf [hereinafter U.N. Fact Sheet].

15. Geneva Int'l Platform, *UN GGE*, https://dig.watch/processes/ungge.

16. U.N. Fact Sheet, *supra* note 14.

17. *Id.*

consensus.[18] Among other things, the GGE recommended a future dialogue on the development on non-binding norms for state use of information and communications technology to reduce risk and protect critical infrastructure.[19]

I think that the very idea of the GGE recommending the development of non-binding norms of appropriate state behavior in cyberspace is fascinating. As international lawyers, we are trained to believe that states articulate appropriate rules governing behavior through treaties—legal documents in which states bind themselves to act in a particular manner. My sense is that the articulation of norms, or best practices, was seen by the GGE as a much less dramatic step that could potentially yield progress in an area of law and behavior that was very much seen as a frontier – where states have been reluctant to identify the legal rules or constraints that apply.

And as Professor Hollis[20] has noted in some of his writings, in some sense the legally binding rules of international law are themselves a species of norms[21]—perhaps more significant because they have been accepted as legally binding, but nonetheless reflecting expectations of state behavior.

A third GGE was established in 2012.[22] Its consensus report acknowledged that international law, in particular the U.N. Charter, is applicable to the cyber-sphere and is "essential to . . . an open, secure, peaceful and accessible ICT [(information and communication technology)] environment."[23] It also acknowledged that "State sovereignty . . . appl[ies] to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory."[24]

A fourth GGE was established in 2014.[25] Its consensus report, issued in 2015, included a number of recommendations for voluntary norms that states should follow in conducting activities in cyberspace. Among others, these norms included four that limit certain state behavior in cyberspace.

First, "states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[26] Second, states should not conduct or

18. *Id.*

19. *Id.*

20. Professor of Law and Associate Dean for Academic Affairs, Temple University Beasley School of Law; Non-Resident Scholar, the Carnegie Endowment for International Peace.

21. *See, e.g.*, *China and the US Strategic Construction of Cybernorms: The Process Is the Product*, 1704 AEGIS PAPER SERIES 1 (2017); *Setting the Stage: Autonomous Legal Reasoning in International Humanitarian Law*, 30 TEMPLE INT'L & COMP. L.J. 1 (2016); *Why State Consent Still Matters: Non-State Actors, Treaties and the Changing Sources of International Law*, 23 BERKELEY J. INT'L L. 137 (2005).

22. *United Nations Group of Governmental Experts' Long-Awaited Report on Maintaining Peace and Stability of the "ICT Environment"*, NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE (Sept. 27, 2013), https://ccdcoe.org/united-nations-group-governmental-experts-long-awaited-report-maintaining-peace-and-stability-ict.html.

23. G.A. Res. A/68/98 at 2 (June 24, 2013).

24. *Id.*

25. G.A. Res. A/70/174 (July 22, 2015).

26. *Id.* at 8.

knowingly support ICT activity that intentionally damages critical infrastructure.[27] Third, states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICTs and the use of harmful hidden functions.[28] And fourth, states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity.[29]

These norms, which the United States played a key role in championing, are voluntary and non-binding, but they reflect in my view a critical breakthrough in establishing an international consensus on responsible international behavior in cyberspace.

The fifth GGE began in 2016 and concluded in June 2017.[30] The group failed to arrive at a consensus.[31] The U.S. representative to the GGE attributed this failure to "the reluctance of a few participants to seriously engage on the mandate on international legal issues."[32] The U.S. representative "call[ed] on all member states to take this seriously in the future and focus on international law."[33] It has been reported that the GGE had debated extensively the application to cyberspace of Article 51 of the U.N. Charter, international humanitarian law, and international law doctrine such as countermeasures.[34]

What can be drawn from this exercise? First, from a U.S. political perspective, it is noteworthy that the negotiating goals of the U.S. representatives to the most recent GGE—which began under the Obama administration and continued under the Trump administration—did not appear to be impacted by the change in administrations. If anything, the U.S. focus on the importance of international law in cyberspace was more pronounced in the U.S. statement issued in June 2017 than it had been at virtually any other point in time in any of the GGE processes. In addition, Deputy National Security Adviser Thomas Bossert praised the "good results" achieved by the GGE in the past, while noting that it was now time to "consider other approaches" and to enforce existing norms.[35] Rather than walking

27. *Id.*

28. *Id.* at 8.

29. *Id.*

30. *UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, GENEVA INTERNET PLATFORM DIGITAL WATCH (Sept. 2, 2016), https://dig.watch/events/un-group-governmental-experts-developments-field-information-and-telecommunications-context.

31. *Id.*

32. Michele G. Markoff, Deputy Coordinator for Cyber Issues, U.S. Dep't of State Office of the Coordinator for Cyber Issues, Explanation of Position at the Conclusion of the 2016-2017 U.N. Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (June 23, 2017).

33. *Id.*

34. Arun M. Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?*, LAWFARE (July 4, 2017, 1:51 PM), https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

35. Thomas P. Bossert, Homeland Security Advisor, The White House, Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017 (June 26, 2017), https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-

away from norms, the United States continues to press for international rules of the road for state behavior in cyberspace.

Second, to a significant extent, the apparent disagreements amongst GGE participants from the most recent GGE appear to be more political than legal. For example, given the GGE's earlier agreement in 2013 that the U.N. Charter applies to state behavior in cyberspace, it is self-evident that Article 51 of the U.N. Charter—governing a state's right of self-defense—would also apply to state behavior in cyberspace.

Third, while the GGE discussions appear to have run their course, we should not overlook the significance of what the GGE has accomplished—slowly, painfully, over the course of many years. The GGE has achieved international acceptance of the application of international law to cyber activities, and agreement on a small number of important norms—independent of legal obligations—that states have identified as a baseline for future behavior. From a U.S. perspective, this includes a norm against state-sponsored cyberattacks on critical infrastructure, which is perhaps more important than ever in light of North Korea's reported capabilities and intentions.

Of course, we should not lose sight of the troubling fact that the most recent GGE could not agree on something as basic as an acknowledgement that general principles of customary international law apply in cyberspace. In my judgment, however, this is more likely the result of political and negotiating tactics and mistrust than a true legal disagreement.

Where next in cybersecurity and diplomacy? The United States—again, through Deputy National Security Advisor Bossert—has indicated its intent to "move forward internationally in meaningful bilateral efforts" with countries like the United Kingdom and Israel.[36]

On a bilateral level, the United States has pursued the identification of additional agreed rules of the road—particularly in discussions with China. One of the most contentious issues in the U.S.-China economic relationship in recent years has been the allegations of economic cyber-enabled espionage that the United States has leveled against China. In 2014, this issue came to a head when the United States took the unprecedented step of indicting five Chinese military officers for conducting economic espionage by hacking into the computer networks of Westinghouse Electric, U.S. Steel, Alcoa, and other U.S. industrial companies to steal trade secrets and other sensitive information for economic benefit.[37]

In 2015, on the eve of President Xi Jinping's visit to Washington, the United States and China agreed in a statement that neither government would support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to

bossert-cyber-week-2017.

36. *Id.*

37. Press Release, Dep't of Justice Office of Pub. Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

companies or commercial sectors.[38] While this statement was not legally binding, it reflected an important political commitment by Presidents Xi and Obama, and this political commitment appears to have made some difference. While economic espionage has not been eliminated, since 2015, outside experts have noted a substantial decrease in Chinese-oriented cyber espionage attacks on U.S. industry. Presidents Xi and Obama also agreed to establish an ongoing dialogue on cybersecurity between the United States and China, and to continue work to identify appropriate norms of state behavior in cyberspace.

The Trump administration has continued this activity. On October 4, 2017, Attorney General Sessions and DHS Secretary Duke met with their Chinese counterparts and confirmed that they would "continue implementation of the consensus reached by" Presidents Xi and Obama in 2015, including continued implementation of the commitment against economic espionage, and continued development of international norms.[39]

Of course, it is important to be clear-eyed about the U.S.-China relationship on cybersecurity. The United States and China have fundamental disagreements on a number of aspects of the appropriate methods of maintaining cybersecurity. For example, the United States has objected strongly to China's recently enacted cybersecurity and related national security laws, which could have a dramatic impact on the operations of U.S. firms in China by "deterring, and in many cases, prohibiting cross-border transfers of information by U.S. firms that are routine in the ordinary course of business."[40] Under the rubric of cybersecurity, China has tightly regulated access to the internet, blocking websites and prohibiting the use of virtual private networks, among other measures.

However, it is noteworthy that despite some fundamental disagreements in approaches to cybersecurity, the United States and China have both publicly signaled the importance of maintaining a dialogue on cybersecurity issues that includes a discussion of appropriate state behavior in cyberspace.

IV. SOVEREIGNTY AND CYBERSPACE

I would like to end by talking a bit about one of the most fundamental and potentially contentious issues relating to cybersecurity and international law that remains unsettled—and that is how concepts of state "sovereignty" apply to, regulate, or restrict state behavior in cyberspace. In the most simplistic terms, we might think of a spectrum of state cyber-related behavior in the territory of another state—each with different international law implications.

On one end of the spectrum is cyber activity that causes significant enough

38. Fact Sheet, The White House Office of the Press Sec'y, President Xi Jinping's State Visit to the U.S. (Sept. 25, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

39. Press Release, Dep't of Justice Office of Pub. Affairs, First U.S.-China Law Enf't and Cybersecurity Dialogue (Oct. 6, 2017), https://www.justice.gov/opa/pr/first-us-china-law-enforcement-and-cybersecurity-dialogue.

40. Tom Miles, *U.S. Asks China Not to Enforce Cyber Security Law*, REUTERS (Sept. 26, 2017, 7:22 AM), https://www.reuters.com/article/us-usa-china-cyber-trade/u-s-asks-china-not-to-enforce-cyber-security-law-idUSKCN1C11D1.

effects to constitute a use of force under international law. For example, think of a cyberattack that results in an explosion at a power plant. There is little debate that these activities should be subject to the normal rules governing the use of force in the territory of another state.

On the other end of the spectrum, consider a cyber activity that has no effect in another territory, or only *de minimus* effects. While not without controversy, in my view, these activities are not prohibited as a matter of customary international law—even if not undertaken with the consent of the other state. There is ample evidence of widespread state practice, taking place on the territory of another state, in activities that have no external effect that may not be condoned by the host state—or that even may be prohibited by the host state's own local laws. I would submit that classic espionage, or intelligence collection, is one such activity.

But what about state cyber activity in this hypothetical middle space, that has some physical effects but not enough to amount to a use of force? This is where the primary debate regarding the international law principle of sovereignty arises. It is not disputed that state sovereignty is applicable to cyber activities—the GGE affirmatively recognized that state sovereignty "appl[ies] to . . . States[‘] [conduct] of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory."[41] But does the principle of sovereignty amount to an international law prohibition on state cyber behavior? This is a subject of significant debate, which has been aired most clearly in the Tallinn Manual 2.0, a cybersecurity legal manual published in 2017 at the invitation of a NATO center by a leading group of international experts.[42] The majority of Tallinn scholars argue that sovereignty is a customary international law rule that establishes a prohibition on state behavior separate and apart from a use of force, or a prohibited intervention in the international affairs of another state—as described in the International Court of Justice's *Nicaragua* case.[43] But others argue that sovereignty, while an important principle that undergirds other prohibitions in the U.N. Charter, does not in and of itself establish a binding prohibition under international law. This issue is fundamental to how states might consider the rules for appropriate behavior in cyberspace.

For example, consider an operation by State A to disrupt an anticipated cyber-attack from State B. Presumably, when an attack is targeted at State A, State A could, consistent with international law, take necessary and proportionate action to stop that attack. While the specific legal theories at play could be complex, I think that under most approaches State A generally would be justified in taking necessary and proportionate action on the territory of State B to thwart the attack, even if it has some other effects on the territory of State B.

In cyberspace, however, the realities of territory and jurisdiction are never as

41. G.A. Res. A/70/174, ¶ 27 (July 22, 2015).

42. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt, ed. 2017).

43. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Merits, Judgment, 1986 I.C.J. Rep. 14, ¶ 212 (June 27); *see* TALLINN MANUAL 2.0, *supra* note 42, at 315, 317, 319–20, 331–32.

simple as this hypothetical would suggest. The attack by State B may take place through operatives located in State C, and via servers located in States D, E, F, and G What does international law, and the principle of sovereignty, have to say about State A's obligations towards States C through G?

Can it be that sovereignty serves as an absolute prohibition on State A taking any action in States C through G without the consent of those states? Or, on the other hand, does international law have nothing to say about State A's obligations to States C through G?

In my view, neither option reflects a satisfactory answer. But this is a critical issue going forward, and it is one that I believe can be assisted by further international law and cybersecurity research and scholarship. Here are a few questions related to this issue that merit further review, in my view.

First, if there is an international law prohibition related to sovereignty—what is the source for the prohibition? To the extent that the prohibition derives from customary international law, how does one account for instances where current persistent and widespread state practice is inconsistent with such a prohibition?

Second, if there is a prohibition, how do the traditional international law doctrines that apply to other areas where states respond to potentially legally wrongful or harmful acts—countermeasures, retorsion, and the obligation to conduct due diligence—impact the legal analysis in cyberspace? Should states think about these concepts differently in cyberspace?

Third, is the intent of State A relevant as an independent measure? In other words, does State A's intent to stop a sub-use-of-force attack on its territory serve as an independent legal justification to act, beyond other traditional international law concepts? If so, what is the source of this justification?

This is one example of an international law issue in cyberspace that has critical security consequences, and that will require diplomacy—coordination between states. Whether in a future GGE or some other fora, these issues require U.S. leadership from a diplomatic and international law perspective.

I will close on this point, and I am happy to take your questions.