August 6-16, 2018
Rio de Janeiro, Brazil

CJI/doc 570/18
9 August 2018
Original: English

# INTERNATIONAL LAW AND STATE CYBER OPERATIONS: IMPROVING TRANSPARENCY

(Presented by Dr. Duncan B. Hollis)

## BACKGROUND

1. Cybersecurity threats have become ubiquitous. Today, cyber-attacks by State and non-State actors—including disruptions of infrastructure, large-scale theft of data and intellectual property, hacking of political actors and election processes—are generating significant losses. These losses are occurring, moreover, across a range of metrics, including national security, human rights, and economics.

2. In 2017, some of the most sensitive hacking tools used by the U.S. National Security Agency and the Central Intelligence Agency were stolen and released on-line.[1] Those tools were repurposed to launch global ransomware attacks like WannaCry, which infected hundreds of thousands of computer networks in 150 countries, with losses totaling up to US$4 billion.[2] Most notably, WannaCry led to the temporary cessation of non-emergency operations at National Health Service hospitals in the United Kingdom.[3] The subsequent NotPetya ransomware attack may have been designed to target Ukraine (and significantly disrupted its hospitals, power companies, airports, and central bank), but it impacted 64 other countries, including several OAS Member States. Companies like FedEx, Maersk, and Merck sustained losses of hundreds of millions of dollars, while key infrastructure was impacted such as Argentina's ports.[4] Malware like "BlackEnergy" has knocked power stations off-line in Ukraine, while a more recent variant known as "Triton" or "Trisis" penetrated the safety controls of large-scale industrial systems in Saudi Arabia in ways that, if not for a small programming error, would have led to the loss of life.[5] Meanwhile, electoral processes in the United States and France have been targeted by hackers, and there are concerns that this practice will be replicated across the Americas.[6] In short, the cybersecurity status quo is poor and deteriorating.

3. Nation States, meanwhile, are increasingly developing their capacities to engage in cyber operations. These efforts include defensive measures and modern iterations of espionage by cyber means. But they also include "offensive" cyber operations that can generate losses of functionality or physical damage to infrastructure and other systems supported by computer networks. At present, some thirty

---

[1] Lily Hay Newman. *The Biggest Cybersecurity Disasters of 2017 So Far,* WIRED, July 1, 2017.
[2] Jonathan Beer, *"WannaCry" ransomware attack losses could reach $4 billion,* CBS NEWS, May 16, 2017.
[3] *Id.*; Damien Gayle et al. *NHS seeks to recover from global cyber-attack as security concerns resurface*, THE GUARDIAN, May 13, 2017.
[4] Newman, *supra* note 1; Conner Forrest, *NotPetya ransomware outbreak cost Merck more than $300M per quarter*, TECHREPUBLIC, Oct. 30, 2017.
[5] *See, e.g.,* Chris Bing. *Trisis has the security world spooked, stumped and searching for answers,* CYBERSCOOP, Jan. 16, 2018; Blake Johnson et al, *Attackers Deploy New ICS Attack Framework "TRITON" and cause Operational Disruption to Critical Infrastructure,* FIREEYE BLOG, Dec. 14, 2017; Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, March 3, 2016.
[6] *See, e.g.,* Adam Nossiter, David E. Sanger, and Nicole Perlroth. *Hackers Came, but the French Were Prepared*, NEW YORK TIMES, May 9, 2017; Kim Willsher, and Jon Henley. *Emmanuel Macron's campaign hacked on eve of French election,* THE GUARDIAN, May 6, 2017.

States have reportedly moved to develop offensive cyber capacities.[7] States appear to favor such operations both as a means to supplement (or even substitute for) traditional means and methods of warfare, but also as a way to consistently engage adversaries short of kinetic armed conflict. In other cases, States have deployed "proxies" to undertake cyber operations, sometimes under the control of the State itself or sometimes simply with more public or private signals of State support.[8]

**International law and cyber operations**

4. How does international law regulate State and State-sponsored cyber-operations? To date, there has only been limited progress in answering this question. In 2013, a United Nations Group of Governmental Experts (the "UN GGE"), which included experts from fifteen governments, adopted a consensus report indicating that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [(information and communication technology)] environment."[9] This view was confirmed by another UN GGE in 2015, which also endorsed a series of voluntary (i.e., non-legally binding) norms for responsible State behavior.[10] These included prohibiting States from peacetime targeting of critical infrastructure or the work of computer security incident response teams (CSIRTs).[11]

5. Unfortunately, much of the GGE's *momentum* was lost in 2017 when the latest GGE failed to generate any report. The twenty governmental experts participating apparently disagreed on whether certain international law regimes (e.g., international humanitarian law, counter-measures, due diligence) applied to State cyber operations.[12] According to the U.S. expert at the negotiations,

> [d]espite years of discussion and study, some participants . . . seem to want to walk back progress made in previous GGE reports. I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions.[13]

6. With the set-back at the GGE, efforts to identify how international law applies to the behavior of States in cyberspace have shifted to other fora. Some efforts have focused on the need for new law, such as Microsoft President Brad Smith's call for a "Digital Geneva Convention."[14] More recently, a

---

[7] Steve Ranger. *US Intelligence: 30 Countries Building Cyber Attack Capabilities*, ZD NET, January 5, 2017.

[8] *See generally* Tim Maurer. *Cyber Mercenaries: The State, Hackers, and Power* (2018).

[9] *See* U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 19, U.N. Doc. A/68/98 (June 24, 2013).

[10] U.N. Secretary-General, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 10, U.N. Doc. A/70/174 (July 22, 2015) ["*2015 GGE Report*"]. The GGE process is, of course, not the only vehicle for inter-State cooperation on cybersecurity. In 2015, for example, U.S. President Barack Obama and Chinese President Xi Jinping announced a "common understanding" on cyberespionage, i.e., a political commitment. They agreed that neither the U.S. nor the Chinese government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors." *See* OFFICE OF PRESS SEC'Y, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT TO THE UNITED STATES (2015). This principle was later endorsed by the G-20. *See* G-20 Leaders' Communiqué, *Antalya Summit*, (Nov. 15–16, 2015), 26, http://www.mofa.go.jp/files/000111117.pdf.

[11] *See 2015 GGE Report, supra* note 10, 13(h), (k).

[12] Arun M. Sukumar. *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well,* LAWFARE, July 4, 2017.

[13] Michele Markoff. U.S. Expert to the Group of Governmental Experts, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security* (June 23, 2017), https://usun.State.gov/remarks/7880.

[14] *See* Brad Smith. *The Need for a Digital Geneva Convention*, MICROSOFT BLOG (Feb. 14, 2017). In the interest of full disclosure, I am currently consulting with Microsoft on this project. To the extent, however, my current proposal focuses on clarifying the existing rules of international law for cyberspace and not proposals for new law, I see these

*Global Commission on the Stability of Cyberspace* has proposed several new "norms" calling on States to promise not to interfere with the "public core" of the Internet or other State's election processes.[15]

7. To date, however, States have done relatively little work collectively to articulate how international law *currently* regulates State behavior in cyberspace. A NATO-funded "independent group of experts" meeting in Tallinn, Estonia produced two manuals on international law and cyberspace. The first *Tallinn Manual* addressed how international law applies to cyberwarfare (i.e., the prohibition on the use of force and international humanitarian law).[16] The second, *Tallinn Manual 2.0*, expanded the treatment to address other areas of international law that regulate State cyber-operations including the duty of non-intervention, sovereignty, and due diligence.[17] Both manuals are important reference works and governments were consulted in their drafting. But for all the expert opinion brought to bear, the *Tallinn Manuals* remain the work of private individuals. They are at best, a "subsidiary" source of international law and cannot be equated to primary sources such as treaties, custom, and general principles.

8. Moreover, as valuable as they are, the *Tallinn Manuals'* contents are often contested or ambiguous. For example, *Tallinn 2.0* describes "sovereignty" not just as a principle that establishes a State's authority to control its territory and population, but a "rule" that can be violated by another State's cyber-operations.[18] *If* sovereignty is a rule, it would establish grounds for a State to complain when another State (or actors for which that State is responsible) conduct cyber operations that impact its civilians or their property. It could, for example, be grounds for reasoning that ransomware like WannaCry or malware like Triton/Trisis breached the sovereignty of victim States.

9. It appears, however, that several States do not (yet) accept the view of sovereignty-as-rule, preferring to identify it as a principle that informs the content of other rules (e.g., the duty of non-intervention) but not as a direct means of regulating State behavior. The U.K. Attorney General adopted this position in a May 2018 speech.[19] The chief lawyer of U.S. Cyber Command has also endorsed the sovereignty-as-principle idea (although writing in a private capacity).[20] As such, there is an open question whether sovereignty even applies to constrain State cyber operations. Similar "existential" debates have arisen about the availability of other proposed "rules" for cyber-operations (e.g., international humanitarian law, due diligence, counter-measures).

10. But even where there is agreement on the application a specific rule to cyber operations, its contours and meaning are often ambiguous. For example, the *Tallinn Manual* experts, while agreeing on sovereignty-as-rule, could not agree on whether a cyber operation that remotely causes a loss of functionality in cyber infrastructure violates the rule if it does not require physically replacing any items in the computer or the infrastructure it supports? Similar questions about how to regulate cyber operations that affect functionality without physical effects have also arisen in competing interpretations of what constitutes an "attack" for purposes of international humanitarian law (i.e., the requirements that States in an armed conflict must not "attack" civilians and must only "attack" military objectives where

---

as separate projects. As such, I do not believe there is a conflict of interest in my working on this topic at the IAJC. That said, I will, of course, defer to the Committee's views on any conflict of interest issues.

[15] *See, e.g.*, Global Comm'n on the Stability of Cyberspace, *Global Commission Proposes Call to Protect the Public Core of the Internet* (Nov. 21, 2017), available at https://cyberstability.org/news/global-commission-proposes-action-to-increase-cyberspace-stability/. For details on the composition and mission of the GCSC, see https://cyberstability.org/.

[16] *See* Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn, Estonia: NATO CCD COE, 2013).

[17] Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn, Estonia: NATO CCD COE, 2017),

[18] *Id.*, at Rule 4 ("A State must not conduct cyber operations that violate the sovereignty of another State.").

[19] *See, e.g.,* Jeremy Wright QC, MP, *Cyber and International Law in the 21st Century*, May 23, 2018, at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[20] *See* Gary Corn, *Tallinn Manual 2.0—Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017).

any civilian losses are proportionate to the military advantage gained). Some, including a majority of the *Tallinn Manual* experts, interpret the "attack" threshold to require physical damage or destruction equivalent to the sorts of kinetic operations that have qualified as attacks previously.[21] Others, such as the International Committee of the Red Cross, argue that the "attack" concept should be expanded given the novel features of information and communication technologies to include losses of functionality even if no physical harm results (i.e., instead of blowing up a power grid, hacking it and temporarily shutting down the system).[22]

11. Thus, there appear to be two distinct problem sets with international law's current application to cyberspace. First, there are "application problems" where it is unclear which rules apply to State cyber-operations. Second, there are "interpretation problems," where assuming a rule applies, its contours and meaning are unclear or disputed.

12. But there is a looming third problem with international law's application to cyberspace as well – what I would call the "accountability problem." Recently, States and other actors have begun to accuse States of responsibility for certain cyber operations (previously, attribution of cyber-attacks was considered either considered too difficult technically or not worth the costs of public disclosure).[23] The United States accused North Korea of responsibility for the hack of Sony Pictures.[24] It later joined with the United Kingdom to accuse North Korea of responsibility for WannaCry as well.[25] Along with a number of other States, these two States have accused the Russian Federation of responsibility for NotPetya.[26]

13. In making these accusations, however, States have clearly avoided invoking international law. None of the accusations mentions let alone attempt to assess how international law regulates such behavior.[27] As a result, there is little accountability for State behavior in cyberspace today.

13a. Taken together, these application, interpretation and accountability problems complicate any attempt to apply international law to cyber operations. Even if a State has its own views on which laws apply and what they mean with respect to its cyber operations, it is not clear that the State targeted by that operation will share these views. This creates a potential for unintended escalations of conflicts (for example, where one State understands its operation to not qualify as a use of force, while the targeted State treats it as such and responds in self-defense). Such state silence, moreover, makes it difficult for customary international law to develop. As States refuse to articulate their views on *opinio juris* in specific cases, it becomes difficult for the customary rules to be identified, let alone applied.

**A modest proposal: asking States for their views on international law**

14. Just because States are reluctant to identify their views on international law with respect to

---

[21] *See Tallinn 2.0, supra* note 17, at 417 (majority accepted the idea that a loss of functionality constitutes damage only if it "requires replacement of physical components").

[22] *See, e.g.,* International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts,* 32nd International Conference of the Red Cross and Red Crescent (Oct. 2015) 40-41 ("2015 ICRC Report").

[23] *See* Duncan B. Hollis, *An e-SOS for Cyberspace,* 52 HARVARD INT'L L. J. 374 (2011).

[24] David E. Sanger and Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES, Dec. 17, 2014.

[25] Nate Lanxon & Tim Ross, *U.K. Blames North Korea for WannaCry Attack on Health Service*, BLOOMBERG, Oct. 26, 2017; *U.S. blames North Korea for 'WannaCry' cyber attack*, REUTERS, Dec. 18, 2017.

[26] Sarah Marsh, *US joins UK in blaming Russia for NotPetya cyber-attack*, THE GUARDIAN, Feb. 15, 2018.

[27] With respect to the Sony Pictures hack, President Obama declined to classify the incident as a violation of international law but referred to it as an act of "cyber-vandalism." Brian Fung, *Obama called the Sony hack an Act of "Cyber-Vandalism*, WASH. POST, Dec. 22, 2014. A recent academic study of the most significant cyber incidents affirms the consistent reluctance of States to apply international law to cyber operations for which a State may be responsible. *See* Dan Efrony and Yuval Shany, *A Rule Book on The Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice*, SSRN (2018).

specific cases does not mean that they must remain silent on international law's application to cyberspace more generally. Whether one agrees with the U.K. Attorney General or not, there is utility in knowing how the United Kingdom views claims of sovereignty as a rule for cyber operations. Similarly, in 2012, the United States offered a series of answers to basic questions about international law's application to cyberspace in a widely read speech by then-Legal Adviser to the State Department Harold Koh.[28] Such statements can contribute to identifying and understanding the relevant international law rules for States in cyberspace. They improve the transparency of how individual States view international law, which—if shared by a sufficient number of other States—may lead to the identification of customary international law. At the same time, these statements have practical importance – they signal to other States, how a State intends to manage and deploy its own cyber operations or respond to those of other States. Such transparency can mitigate the potential for unintended consequences or escalations arising from cyber operations by States or those whose behavior may be attributed to a State.

15. Thus, I would propose that the IAJC undertake a new project – soliciting, compiling, and publicizing Member State views on international law's application to cyber operations. This would build on ad hoc statements that have been issued by government officials to date. But instead of having these views spread out over time and location, our Committee could compile a collection of Member State responses on some of the most important international legal questions in an area – cybersecurity – that has become a national priority for all States in the region.

16. I believe, moreover, that the OAS is uniquely situated among international organizations to undertake such a project. As noted, global efforts at the United Nations have faltered because certain States have fundamentally different visions of cyberspace and the role of States therein. Other regional organizations, such as the OSCE and the Council of Europe, have stalled due to similar disagreements among Member States. In contrast, OAS Member States all share a commitment to democratic values and the rule of law. As such, the OAS is perhaps the one regional international organization that could offer a collective set of views on how international law applies to cyber operations. To the extent Member State responses conform to existing statements on international law offered at the UN GGE or elsewhere, these responses would make an important contribution by signaling that such statements enjoy broad support. And where OAS Member States offer consistent views on international legal issues not previously articulated, they can make a strong case for treating such views as reflective of customary international law in the region, if not across the globe.

17. That said, I do not anticipate Member States will always offer similar answers to key, outstanding questions surrounding international law and cyber operations. Nonetheless, there is still value in identifying cases where Member States offer inconsistent views. It will be possible to map areas of both convergence and divergence. Knowing where States disagree can highlight areas in need of further dialogue or attention, whether to close these gaps, articulate clarifications, or to seek modifications to ensure that international law can be more effective in regulating actual State behavior in cyberspace.

18. In sum, I seek the Committee's approval to draft and send Member States a questionnaire, asking for their official views on some of the key questions that have arisen with respect to the application of international law to operations in cyberspace by States or by those actors for whom a State might be internationally responsible. I am also seeking the Committee's approval to raise this subject with the Foreign Ministry's Legal Advisers during our August 15, 2018 meeting. The receptivity of these Legal Advisers to the idea of a questionnaire will be an important bellwether to the success of the project proposal as a whole. That dialogue may also identify certain topics that are (or are not) fruitful for attention as part of any effort to improve the transparency of international law's application in cyberspace.

19. To facilitate the discussion, I am attaching a draft list of 20 questions that I propose the

[28] *See* Harold Hongju Koh. Legal Advisor U.S. Department of State, *International Law in Cyberspace,* USCYBERCOM Inter-Agency Legal Conference, Sept. 18, 2012, *available at* https://2009-2017.State.gov/s/l/releases/remarks/197924.htm.

Committee pose to Member States. They parallel the sorts of questions on which some States (e.g. the United States) have already offered views. They are, however, both more detailed and numerous than those the Committee usually produces. Nonetheless, I believe they are all worth asking. Still, it will be important to communicate to Member States that their answers themselves are the desired product of the Committee's work. The value of this project lies in having States be more transparent in how they understand international law to operate in this space. Thus, we will need to work as a Committee – in concert with the Department of International Law – to engender more (and more detailed) responses than we have received in other contexts.

20. If the Committee approves this topic, I would work with the Secretariat to identify a set of appropriate questions that could be posed to Member States this Fall such that the responses could be collected and analyzed by this Committee next year, and, with the General Assembly's approval, publicized within the region and beyond.

**[DRAFT]**

# 20 QUESTIONS FOR MEMBER STATES ON INTERNATIONAL LAW AND CYBER OPERATIONS

**The application of international law generally**

1. Do existing rules of international law apply to cyberspace?
2. Are there areas where the novelty of cyberspace excludes the application of international law?

**Cyber operations and the use of force**

3. Can a cyber operation alone qualify as a use of force or the threat of a use of force? Under what conditions might a cyber operations qualify as "force"?
4. Can a cyber operation alone qualify as an armed attack justifying a response in self-defense under Article 51 of the UN Charter or Article 22 of the OAS Charter?
    i. Under what conditions might a cyber operation qualify as an armed attack?
    ii. Could an operation do so if it disrupted critical infrastructure without causing the sorts of violent effects that have qualified as an armed attack in the kinetic context?
5. Can a non-State actor's cyber operation qualify as a use of force or an armed attack? What level of control or involvement must a State have in order to be regarded as responsible for such an operation under international law?

**Cyber operations and international humanitarian law (IHL)**

6. Can cyber operations alone constitute an armed conflict? Is there some level of intensity required of a cyber operation to do so?
7. Where there is an armed conflict, do IHL's rules apply to a State's cyber operations?
8. When do IHL's rules apply to cyber operations conducted by a non-State actor?
9. When would a cyber operation qualify as an attack under IHL?
    i. Can a cyber operation qualify as an attack where it does not cause any direct physical harm to the targeted computer system or network?
    ii. Would ransomware, for example, ever qualify as an attack?
    iii. Can a loss of functionality alone constitute an attack?
    iv. Does data alone qualify as a military objective subject to attack under IHL?
10. When is a computer system or network regarded as a military objective? Can a computer system or network that is primarily used for civilian purposes qualify as a military objective?

**The duty of non-intervention**

11. Does the duty of non-intervention apply to cyber operations by a State or those actors for whom a State would be internationally responsible?
12. Which information and communication technologies or infrastructure are protected by the duty of non-intervention (that is, which qualify as part of the *domain réservé*)?
13. When would a cyber operation constitute coercion for purposes of the duty of non-intervention?
14. Can cyber operations that target political campaigns or a State's electoral processes violate the duty of non-intervention? In what circumstances might they do so?

**Sovereignty**

15. Is sovereignty a rule of international law that prohibits States from engaging in specific cyber operations?

16. If so, which cyber operations might be restricted by this rule? Could operations having no direct, physical effects in a State's territory nonetheless violate its sovereignty?

17. If sovereignty qualifies as a rule of international law, can a non-State actor's cyber operation violate a State's sovereignty?

**Due Diligence**

18. Does due diligence qualify as a rule of international law that States must follow in exercising their sovereignty over their territory and nationals?

19. If so, under what circumstances would a State be expected to exercise due diligence with respect to behavior by (a) other States in its territory; (b) non-State actors, including (c) its own nationals?

**Other rules of international law**

20. Are there other rules of international law that are important to highlight in assessing the regulation of cyber operations by States or actors for which a State is internationally responsible?

*** * ***