THE TALLINN MANUAL 2.0: HIGHLIGHTS AND INSIGHTS

ERIC TALBOT JENSEN*

ABSTRACT

Malicious cyber activities are pervasive in the lives of individuals and in the national security discussions of national governments across the globe. It is rare for a day to pass without some cyber event reaching the national news. These malicious cyber activities are attributed to both state and non-state actors such as transnational criminal groups, terrorist organizations, and individuals.

In response to this widespread phenomenon, including a specific major cyber incident in Estonia in 2007, the Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia hosted a multi-year process designed to provide the views of a group of renowned experts on the application of international law to cyber activities. The first Tallinn Manual dealt with the law applicable to armed conflict. The second, and recently published, Tallinn Manual (known as Tallinn 2.0) deals with a much broader type of cyber operations—those both in and out of armed conflict.

This Article briefly summarizes the key points in the Tallinn Manual 2.0, including identifying some of the most important areas of non-consensus among the Experts who wrote the Manual. The Article then offers some insights into where international law on cyber operations will need to go in the future.

* Professor of Law, Brigham Young University Law School. Professor Jensen served as a member of the International Group of Experts on both Tallinn 1.0 and Tallinn 2.0.

I. INTRODUCTION

Malicious cyber activities have become a normal part of our lives. Not only do cyber events appear regularly in the news,[1] but they also capture the imagination of viewers watching movies[2] and television,[3] and provide endless intrigue in literature.[4] Many of these fictional scenarios involve major cyber breaches that lead to catastrophic consequences, often involving armed conflict between countries.[5]

Fortunately, such a cyber scenario has not yet occurred in real life. Instead, the vast majority of malicious cyber activity has taken place far below the threshold of armed conflict between states, and has not risen to the level that would trigger such a conflict. Rather, the majority of cyber activities so prevalent in the news involve the stealing of corporate secrets,[6] the spreading of false information,[7] or the breach of

1. *See, e.g.*, Juliet Eilperin & Adam Entous, *Russian Operation Hacked a Vermont Utility, Showing Risk to U.S. Electrical Grid Security, Officials Say*, WASH. POST (Dec. 21, 2016), https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.8cf73411023c.

2. BLACKHAT (Legendary Entertainment 2015); Elizabeth Weise, *Eight All-time Great Hacking Movies*, USA TODAY (Jan. 14, 2015, 12:08 PM), https://www.usatoday.com/story/tech/2015/01/14/hacking-movies-list-cyber-blackhat/21713327/.

3. *See, e.g.*, *CSI: Cyber*, CBS, http://www.cbs.com/shows/csi-cyber/ (last visited June 7, 2017) (American television drama concerning police investigations of cyber crimes); *Good or Bad, Here Are 4 New Hacker TV Shows That Debuted in 2015*, CLOUDBRIC, https://www.cloudbric.com/blog/2015/07/good-or-bad-here-are-4-new-hacker-tv-shows-debuted-in-2015/ (last visited June 1, 2017).

4. *See, e.g.*, Diane Biller, *Here Are 21 Essential Cyberpunk Books That You Absolutely Should Read*, GIZMODO (Jan. 2. 2016, 4:15 PM) https://www.gizmodo.com.au/2016/01/the-essential-cyberpunk-reading-list/.

5. One of the first such movies was "War Games", the story of a defense computer gone wrong that threatens to initiate nuclear war. WAR GAMES (United Artists 1983).

6. *See, e.g.*, James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN TECH (Oct. 8, 2015, 3:28 AM), http://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/.

7. Rebecca Greenfield, *Look What the Hacked AP Tweet About White House Bombs Did to the Market*, THE ATLANTIC (Apr. 23, 2013), https://www.theatlantic.com/technology/archive/2013/04/hacked-ap-tweet-white-house-bombs-stock-market/315992/.

government computers in an attempt to steal state secrets.[8]

Nevertheless, the significance of cyber hacking has become a reality for millions of individuals whose personal information has been compromised through cyber means.[9] The prevalence of these cyber events, along with the risks they raise to states individually and to the international community as a whole, have forced both states[10] and multinational organizations[11] to take notice and seek solutions. Among those multinational organizations is the North Atlantic Treaty Organization (NATO) whose Cooperative Cyber Defense Center of Excellence (CCD COE)[12] in Tallinn, Estonia, helped facilitate the original Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0)[13] and the newly released Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[14] The substance of Tallinn 1.0 appears in Tallinn 2.0, though slightly altered to reflect points of clarification since its original publication.

This Article will briefly summarize the key points in the Tallinn Manual 2.0 (the Manual), including identifying some of the most important areas of non-consensus among the legal experts who wrote

8. *See, e.g.*, Ryan O'Hare, *China Proudly Debuts its New Stealth Jet it Built 'by Hacking into US Computers and Stealing Plans'*, DAILY MAIL (Nov. 1, 2016, 06:57 EDT), http://www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes-public-debut.html (alleging the new Chinese aircraft borrowed heavily from stolen plans for US aircraft).

9. *See* Sam Thielman, *Yahoo Hack: Ibn Accounts Compromised by Biggest Data Breach in History*, THE GUARDIAN (Dec. 15, 2016, 7:23 PM), https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

10. *See* Statement of James R. Clapper Before the Senate Armed Services Committee, Worldwide Threat Assessment of the US Intelligence Community 1–4 (February 9, 2016), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-26-15.pdf; *see also* U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY 2011-2016: ANNUAL REPORT (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

11. *See* Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (July 22, 2015) [hereinafter UN Doc. A/70/174]; Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (June 24, 2013) [hereinafter UN Doc. A/68/98].

12. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE), https://ccdcoe.org/ (last visited June 1, 2017).

13. TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2012) [hereinafter TALLINN MANUAL 1.0].

14. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

the Manual. The Article will also attempt some insights into where international law on cyber operations will need to go in the future.

II. The Process

Both Tallinn Manuals were written by groups of international legal experts (the Experts)[15] gathered by the CCD COE and Michael N. Schmitt,[16] a prominent global cyber expert. The first group included law of armed conflict (LOAC) experts primarily from the Western Hemisphere. In response to criticism, the international group of experts for Tallinn 2.0 was broader both in origin (including members from Thailand, Japan, China, and Belarus) and substantive expertise (including experts in human rights, space law, and international telecommunications law). The International Committee of the Red Cross (ICRC) was invited to send observers to both groups as were other states and organizations.

The intent of the project was never to make law or to produce a manual that would have the force of law. As the introduction makes clear:

> Ultimately, Tallinn Manual 2.0 must be understood only as an expression of the opinions of the two International Groups of Experts as to the state of the law . . . . This Manual is meant to be a reflection of the law as it existed at the point of the Manual's adoption by the two International Groups of Experts in June 2016. In is not a 'best practices' guide, does not represent 'progressive development of the law', and is policy and politics-neutral. In other words, Tallinn Manual 2.0 is intended as an objective restatement of the *lex lata*.[17]

The processes differed somewhat in originating the substance of the Manuals, but in both cases, the procedure for finalizing the substance was the same. Rules, which appear in bold, black letters in both Manuals, required consensus, so all the experts had to agree on each rule. Following each Rule in the Manual is a fairly extensive commen-

---

15. The author was a member of both International Groups of Experts. For the members of the International Group of Experts and the other participants involved in the publication of the Tallinn Manual 1.0, see Tallinn Manual 2.0, *supra* note 14, xix–xxii. For those involved in the publication of the Tallinn Manual 2.0, see *id.* at xii–xviii.

16. *Faculty: Michael N. Schmitt*, U.S. Naval War College, https://usnwc.edu/Faculty-and-Departments/Directory/Michael-N-Schmitt (last visited June 1, 2017).

17. Tallinn Manual 2.0, *supra* note 14, at 2–3.

tary, produced in normal font for clarity from the rule. The Commentary provides definitions, explanations of the rules, details of how the rule is to be applied, scenarios and examples, and most importantly, it identifies where the Experts could not agree on a particular aspect of the Rule.

For example, the Experts agreed that prescriptive nationality jurisdiction applied to a state's nationals even when overseas, but did not agree on whether that individual's data was subject to extraterritorial enforcement jurisdiction of the national's state. The Rule, upon which all the Experts agreed states that "A State may exercise extraterritorial prescriptive jurisdiction with regard to cyber activities: (a) conducted by its nationals; . . . "[18] but the commentary to a later Rule states:

> It should be noted that a few Experts distinguished between prescriptive jurisdiction over the cyber activities of nationals and jurisdiction over data created during those activities. They were of the view that the jurisdiction of the State over data often cannot be equated to its jurisdiction over the cyber activities of its nationals. All Experts agreed, however, that the State where the data is located will possess full jurisdiction over the data.[19]

This passage points out another key part of the process—how the Manual deals with lack of consensus. When the Experts disagreed, the Manual notes that disagreement in several ways. Where the group was divided into a majority and a minority,[20] the Manual makes note of that. At times when the group was further divided, the Manual will often use the description of "[s]ome of the experts"[21]—usually meaning several or a small minority. At times, the Manual will note that "[a] few of the Experts"[22] took a particular view. That normally means only one or sometimes two of the Experts held that view. And finally, there

---

18. TALLINN MANUAL 2.0, *supra* note 14, at 60 r. 10(a).

19. *Id.* at 63, ¶ 8.

20. *See, e.g.*, *id.* at 19, ¶ 7 ("In this regard, the Experts divided over the unique case of cyber espionage (Rule 32) by one State that is conducted while physically present on the territory of another State. The majority took the position that the activity violates this Rule.").

21. For example, with respect to the use of countermeasures, the TALLINN MANUAL 2.0 provides: "However, some of the Experts took the opposite position. By their approach, for instance, an injured State would be required to attempt available acts of cyber retorsion before taking cyber countermeasures if they would likely to cause the responsible State to comply with its obligations." *Id.* at 118, ¶ 4.

22. For example, concerning the application of human rights, the TALLINN MANUAL 2.0 provides: "A few of the Experts took the position that so long as the exercise or enjoyment of a

were views that were legitimate views that the Experts knew existed, but that none of the Experts held. In those cases, the Manual will normally state "the Experts acknowledged a view."[23]

As the Experts completed the text for Tallinn 2.0, the Dutch government initiated a process of several meetings with states during which they could review and comment on the substance of the Manual before it was finalized. More than fifty states took advantage of those meetings, including all the permanent members of the Security Council. This input, while not necessarily included in the Manual because the Manual is the view of the Experts, provided invaluable insights into how states viewed the implementation of international law with respect to cyber operations.

Additionally, select portions of the Manual were sent out to "peer reviewers" in order to get their input as well. Once all of the external input was received, from both states and peers, it was presented to the Experts for consideration as the draft rules and commentary were finalized.

This extensive process, particularly with respect to Tallinn 2.0, allowed for the consideration and potential adoption of a far wider set of views and expertise than is gathered in any other single source. Thus, the Tallinn Manuals will provide a unique and comprehensive statement on the international law applicable to cyber operations.

III. The Manual

The Manual is divided into four parts. Part I deals with general international law and cyberspace. Part II covers specialized regimes of international law and cyberspace. Part III concerns international peace and security and cyber activities, which is drawn mostly from Tallinn 1.0. And Part IV is the rest of Tallinn 1.0 and applies to the law of cyber armed conflict. As Tallinn 1.0 has already been extensively commented on, this Article will draw exclusively on Parts I and II and a small portion of Part III.

A. *Sovereignty*

The Manual begins with a discussion of sovereignty and makes the point in its first rule that "[t]he Principle of Sovereignty applies to

---

human right in question is within the power or effective control of a State, that State has power or effective control over the individual with respect to the right concerned." *Id.* at 185, ¶ 10.

23. For example, in discussing the inviolability of diplomatic and consular premises, the Tallinn Manual 2.0 provides: "The Experts acknowledged a view, which none of them held, by which the inviolability of the premises of a diplomatic mission is absolute." *Id.* at 214,¶ 7.

cyberspace."[24] The subsequent two rules differentiate between internal and external sovereignty,[25] and Rule 4 says that "[a] State must not conduct cyber operations that violate the sovereignty of another State."[26]

The assumption underlying the Expert's conclusion in Rule 4 is that sovereignty is a rule of international law, the violation of which is an internationally wrongful act. The commentary to Rule 4 states:

> In the cyber context, therefore, it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there. For example, if an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place.[27]

This "sovereignty-as-rule" approach is not universally accepted. Colonel Gary Corn, the U.S. Cyber Command senior legal advisor, argues:

> An opposing view holds that sovereignty is a baseline principle of the Westphalian international order undergirding binding norms such as the prohibition against the use of force in Article 2(4) of the UN Charter, or the customary international law rule of non-intervention, which States have assented to as an exercise of their sovereign equality.[28]

Under this approach, sovereignty is reflected in rules such as the prohibition on the use of force and the rule against intervention, but is not an enforceable rule in and of itself.

There is also a third view, forwarded by this paper, of the application of sovereignty to cyber operations. By this view, sovereignty is a prin-

---

24. *Id.* at 11 r. 1.

25. TALLINN MANUAL 2.0 Rule 2 provides that "A State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations." *Id.* at 13 r. 2. Rule 3 provides that "A State is free to conduct cyber activities in its international relations subject to any contrary rule of international law binding on it." *Id.* at 16 r. 3.

26. *Id.* at 17 r. 4.

27. *Id.* at 19, ¶ 6.

28. Gary Corn, *Tallinn Manual 2.0–Advancing the Conversation*, JUST SECURITY (Feb. 15, 2017, 8:41 AM), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more-37812.

ciple that depends on the domain and the practical imperatives of states and is subject to adjustment in interstate application. Briefly contrasting how sovereignty is treated in the territorial based regimes of air, land, sea, and space illustrates the point.

Historically, sovereignty predates the establishment of the modern state and originates in the Prince as Sovereign.[29] With the rise of the modern state, international law has been formed by states applying the doctrine of sovereignty to particular sets of facts or instances of state interaction. For example, considering land territory, sovereignty has been applied differently to diplomats and spies from other state nationals. With respect to espionage, states have not found espionage to be a per se violation of sovereignty, even when those actions take place in and/or have effects in another state. States routinely outlaw the methods of espionage as a matter of domestic law, but not as a violation of sovereignty. Similarly, long before the Vienna Convention on the Law of Treaties[30] was promulgated, customary international law provided immunities to diplomatic premises and persons on the territory of other states. Though states adapted the application of the principle of sovereignty with respect to land territory differently in these two cases, they support the assertion that sovereignty is a principle that gets applied based on the practical imperatives of states, rather than as a uniform rule of international law.

Contrasting the application of sovereignty in the domains of air, space, and sea is also instructive.[31] In these cases, sovereignty has been

---

29. *See generally* PHILIP BOBBITT, THE SHIELD OF ACHILLES (2002) (tracing the doctrine of sovereignty through history to the modern application).

30. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331, 8 I.L.M. 679.

31. The U.S. Department of Defense's Assessment of International Legal Issues in Information Operations helpfully contrasts sovereignty as applied to the domains of air, space, and sea:

> The international community ordinarily does not negotiate treaties to deal with problems until their consequences have begun to be felt. This is not all bad, since the solution can be tailored to the actual problems that have occurred, rather than to a range of hypothetical possibilities. One consequence, however, is that the resulting law, whether domestic or international, may be sharply influenced by the nature of the events that precipitate legal developments, together with all their attendant policy and political considerations.
>
> The development of international law concerning artificial earth satellites provides a good example. If the nations had sat down with perfect foresight and asked themselves, "Should we permit those nations among us that have access to advanced technology to launch satellites into orbit that will pass over the territory of the rest of us and take high-resolution imagery, listen in our telecommunications, record weather information,

applied differently by the international community depending on the practice of states across these domains, resulting in disparate legal paradigms. The lack of legal consistency across these domains makes the formulation of a rule that will apply to cyberspace especially difficult. It appears, based on state practice to date, that states are applying sovereignty with respect to cyberspace in a way that does not preclude cyber activities on the infrastructure and territory of another state to include actions taken by one state that do not impinge on the inherently governmental functions of another state.

What seems clear is that, as stated by former Department of State Legal Advisor Brian Egan, the international community is currently "faced with a relative vacuum of public State practice."[32] Mike Schmitt echoed this at the U.S. launch of the Tallinn Manual 2.0. When asked what part of the Manual is most likely to change in the next five years, he answered that he thought it would be that states would need to clarify their positions on sovereignty.[33] Again, as Brian Egan argued, "[s]tates should publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent

---

> and broadcast information directly to telephones and computers within our borders?", a very restrictive regime of space law might have resulted. Instead, what happened was that the first satellites launched by the Soviet Union and the United States were seen as entirely benign devices engaged in scientific research, and it was also perfectly clear that no nation had the capability to interfere with them as they passed over its territory. In these circumstances, it quickly became accepted customary international law, soon enshrined in the Outer Space Treaty, that objects in orbit were beyond the territorial claims of any nation, and that outer space is available for exploitation by all.
>
> The history of space law contrasts sharply with that of air law. Much of the early development of heavier-than-air aviation coincided with the First World War, during which the military power of aircraft for intelligence gathering, attacking ground forces, and bombing enemy cities was clearly demonstrated. The result was a highly restricted regime of air law in which any entry into a nation's airspace without its permission was to be regarded as a serious violation of its sovereignty and territorial integrity.

U.S. DEPARTMENT OF DEFENSE OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 2 (2d ed. Nov. 1999).

32. Brian Egan, Legal Adviser to the Department of State, Remarks on International Law and Stability in Cyberspace at Berkeley Law 5 (Nov. 10, 2016), https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf [hereinafter Egan Remarks].

33. Michael N. Schmitt, Remarks at the Atlantic Council Meeting: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (Feb. 8, 2017), http://www.atlanticcouncil.org/blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace (providing an overview of the general discussion). The specific point is based on a question posed to Schmitt by the author at the Meeting.

possible in international and domestic forums."[34] It is only through the elucidation of state positions on the interaction of sovereignty and cyber capabilities that this question will be answered.

B. *Due Diligence*

Due diligence is not a substantive provision of international law, but rather the standard that states must apply in preventing their territory from being used to cause transboundary harm.[35] As stated in Rule 6 of the Tallinn Manual, "a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."[36]

There are several important aspects to this rule. First, the Rule recognizes that states' obligation to apply due diligence is in fact a rule of international law. When that standard must be applied and to what degree is still a matter of discussion, but the fact that the rule exists and applies to states was uncontested with the Experts.[37]

States are not required to remedy all transboundary harm; only that harm resulting in serious adverse consequences. Some level of harm is assumed to be below the threshold that would trigger the due diligence principle.[38] Despite using this language in the Rule, the Tallinn Experts could not fully describe what "serious adverse consequences" meant. In fact, they concluded that international law on this point was unclear.[39] However, the Experts did argue that no "physical damage to objects or injuries to individuals" was required.[40]

For a state to be responsible for applying due diligence to prevent transboundary harm, the state must have knowledge of the harm. That knowledge may be constructive knowledge if the state, in the normal course of events, would or objectively should have known about the harm.[41] However, such a view does not require a state to take preventive measures with its cyber infrastructure,[42] or even monitor infrastruc-

34. Egan Remarks, *supra* note 33, at 7.

35. TALLINN MANUAL 2.0, *supra* note 14, at 30 r. 6.

36. *Id.* r. 6.

37. *Id.* at 31, ¶ 4.

38. *Id.* at 36, ¶ 22.

39. *Id.* at 36–37, ¶ 25 n. 48.

40. *Id.* at 37–38, ¶ 28.

41. *Id.* at 41, ¶ 39.

42. *Id.* at 439, of the to work erts and the other participants involved in the publication of the 44–45, ¶ 7.

ture in an effort to be apprised of any potential transboundary harm.[43]

At the point where a state knows of the transboundary harm, it is required to take "all measures that are feasible in the circumstances to put an end to the cyber operations."[44] In other words, the state must take measures that are "reasonably available and practical,"[45] though the means whereby this is accomplished is at the discretion of the state from which the harm is emanating.[46]

States are not generally fond of the due diligence principle because it places some amount of responsibility on them. In the United Nations Group of Governmental Experts (UN GGE), states were only willing to admit that they "should" exercise due diligence, rather than that they "must" as the Rule states.[47] However, when analyzed in conjunction with the previous principle of sovereignty, even the standard proposed by the Experts leaves a large gap where victims of cyber harm are left with few remedies.

For example, assume that a terrorist organization in State A is conducting harmful cyber activities against entities in State C through State B. Both States A and B have no affirmative obligation until they know the harm is taking place. Because they have no obligation to monitor or prevent, States A and B are likely to come to the knowledge of the harm only after State C has suffered sufficient harm to conduct computer forensics and determine where the harm is coming from.

Even when State C knows from where the harm is originating, it is unable to take any proactive measures, such as countermeasures which will be discussed below, because the harm is being caused by a non-state actor. This leaves State C completely reliant on State A's and State B's acceptance of the assertion by State C, State A's and State B's determination that it is true and that the harm is coming from within their territory (including whatever time and process they feel is necessary to ascertain the facts), their analysis of what would be feasible to do to block the harm, and their determination of what feasible measures they will implement to stop the transboundary harm.

Some might argue in response that this is no different than the application of the due diligence principle in other areas of international law, such as international environmental law. However, the

---

43. *Id.*

44. *Id.* at 43 r. 7.

45. *Id.*, ¶ 2.

46. *Id.* at 44, ¶ 6.

47. *See* UN Doc. A/70/174, *supra* note 11, ¶¶ 13(c), 28(e); ¶ 23, UN Doc. A/68/98, *supra* note 11, ¶ 23.

fundamental differences include that environmental transboundary harm is often more transparently manifest and often easier to allocate responsibility. Additionally, environmental harm often has effects in the host state on its way to the victim state, providing greater encouragement for the host state to take action. Environmental harm is usually contiguous and involves neighbors which might share more vested interests. And finally, there is little evidence of states using proxies to cause environmental harm to their neighbors, leaving little incentive to deny the harm or delay the remedy. However, with malicious cyber activities, the situation is quite different, with a host of allegations that states use proxies to conduct cyber activities, specifically with the intent of being able to deny attribution.[48]

Given the fact that sovereignty is one of the principles most under pressure and due diligence is one of the principle means of applying pressure, this is an area of great interest to follow over the next few years as greater state practice develops.

C. *Jurisdiction*

The chapter of the Manual on jurisdiction encompasses six rules and extensive commentary. Jurisdiction is defined as "the competence of States to regulate persons, objects, and conduct under their national law, within the limits imposed by international law."[49] The first rule on jurisdiction states, "[s]ubject to limitations set forth in international law, a State may exercise territorial and extraterritorial jurisdiction over cyber activities."[50] This means that "in principle, cyber activities and the individuals who engage in them are subject to the same jurisdictional prerogatives and limitations as any other form of activity."[51]

The Manual addresses the three traditional types of jurisdiction—prescriptive, enforcement, and adjudicative—and discusses key aspects of each one. With respect to prescriptive jurisdiction, the Manual explains that states are basically unfettered with respect to prescriptive jurisdiction within their sovereign territory and can exercise prescrip-

48. *See* Tim Mauer, *Cyber Proxies and the Crisis in Ukraine*, *in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE, NATO CCD COE 79, 81–82 (Kenneth Geers ed., 2015) https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf; Tim Maurer, *'Proxies' and Cyberspace*, 21 J. CONFLICT & SECURITY L. 383 (2016); Luke Penn-Hall, *The Problem with Proxies*, THE CIPHER BRIEF (July 21, 2016), https://www.thecipherbrief.com/article/tech/problem-proxies-1092.

49. TALLINN MANUAL 2.0, *supra* note 14, at 51, ¶ 1 (internal citations omitted).

50. *Id.* r. 8.

51. *Id.*, ¶ 2.

tive jurisdiction extraterritorially (meaning based on either location of the cyber activity or its effects) if based on one of the traditional bases for extraterritorial jurisdiction.[52]

Rule 9[53] discusses territorial jurisdiction and confirms that both subjective and objective territorial jurisdiction apply to cyber activities. In most cases, this was a non-controversial rule. However, the group split on the question of cyber activities with only a minimum connection, such as transiting data. Some of the group thought a state could exercise jurisdiction on transiting data and others did not think so.[54] This point is illustrated by an example from the Manual.

Consider a scenario where data from a cyber operation initiated in State A transits State B on its way to State C, where it actually has effects. State A can exercise prescriptive territorial jurisdiction as the state where the cyber activity originated; State C can as well as the state where the effects occur; but can State B exercise jurisdiction? The Experts split on that question.[55] In determining an answer, of course it is important to resolve who determines what is a minimum connection, or de minimis. And, of course, however this question is resolved does not prejudice a state from exercising other bases of jurisdiction, such as nationality.[56] Further, this determination has important repercussions on the issue of due diligence discussed above.

Rule 10[57] acknowledges that states can also assert extraterritorial

---

52. *Id.* at 51–52, ¶ 3.
53. TALLINN MANUAL 2.0 Rule 9 provides that a:

> A State may exercise territorial jurisdiction over:
>
> (a) cyber infrastructure and persons engaged in cyber activities on its territory;
> (b) cyber activities originating in, or completed on, its territory; or
> (c) cyber activities having a substantial effect in its territory.

Id. at 55 r. 9.
54. *Id.*, ¶¶ 2–3.
55. *Id.* at 55–56, ¶ 4.
56. *Id.* at 56, ¶ 55.
57. TALLINN MANUAL 2.0 Rule 10 provides that:

> A State may exercise extraterritorial prescriptive jurisdiction with regard to cyber activities:
>
> (a) conducted by its nationals;
> (b) committed on board vessels and aircraft possessing its nationality;
> (c) conducted by foreign nationals and designed to seriously undermine essential State interests;
> (d) conducted by foreign nationals against its nationals, with certain limitations; or
> (e) that constitute crimes under international law subject to the universality principle.

Id. at 60 r. 10.

jurisdiction through nationality, the protective principle, passive personality, and universality with respect to cyber activities outside their territory. With respect to nationality jurisdiction, one of the interesting questions that remains unresolved concerns the cyber activities of a state's nationals and whether a state can exercise jurisdiction only over the individual abroad or also the data created by the individual.[58] In other words, if the national of State A creates data in State B, it is unclear if State A can exercise jurisdiction over that data as well as the individual.

Rule 11 deals with enforcement jurisdiction.[59] As with prescriptive jurisdiction, states can exercise enforcement jurisdiction in their territory but have a more limited ability to exercise extraterritorial enforcement jurisdiction, such an exercise is generally allowed only upon consent of the territorial state. This is also one of the areas where cyber activities present a number of interesting issues.

Rule 11 presents a narrow view of enforcement jurisdiction and there are certainly some who have argued for a broader view. The Tallinn Manual view is that international law, including specific treaties such as the law of the sea, outer space, and treaties concerning aviation activities, might support the exercise of enforcement jurisdiction abroad. It was the opinion of the Experts that where these grants of jurisdiction occur, they would include cyber related activities.[60] In fact, some treaties may specifically invoke certain extraterritorial enforcement privileges, such as the Convention on Cybercrime.[61]

Given the nature of cyber data, the Tallinn Group (Group) acknowledged that there may be times when it is unclear in which state data or other digital evidence resides. The Group determined that international law currently doesn't address this issue clearly so the Group was unable to come to any kind of consensus on that case.[62] Assumedly, in

---

58. *See id.* at 63, ¶ 8.

59. TALLINN MANUAL 2.0 Rule 11 provides that:

> A State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects and cyber activities on the basis of:
>
> (a) a specific allocation of authority under international law; or
>
> (b) valid consent by a foreign government to exercise jurisdiction on its territory.

Id. at 66 r. 11.

60. *Id.* at 67, ¶ 3.

61. Convention on Cybercrime, Council of Europe, E.T.S. 185, Nov. 23, 2001 (entered into force July 1, 2004), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

62. TALLINN MANUAL 2.0, *supra* note 14, at 68, ¶ 8.

such a case, a state which decided to exercise its enforcement jurisdiction would do so subject to some amount of risk.

The Experts also noted that there may be difficulty in assessing whether electronic data that is widely available on the internet, but hosted on servers in another state is an exercise of territorial or extraterritorial enforcement jurisdiction. Ultimately, the Group decided that it was an exercise of territorial jurisdiction because the data is available in the concerned state. This is true even if the data is non-public and password-protected as long as it is accessed from the state's territory.[63] In contrast, data that may be accessible via the internet but is not intended to be available to individuals in the concerned state requires an exercise of extraterritorial enforcement jurisdiction and either consent or specific authorization by international law.[64]

The Manual also recognizes that adjudicative jurisdiction is generally co-extensive with prescriptive jurisdiction but its exercise may be limited by the consent of a territorial state.[65] With respect to situations of military members abroad, Status of Forces Agreements often have specific grants of consent to the sending state to allow adjudicative jurisdiction over members of the force. Other agreements might have similar effects in specific situations.[66]

Of course, none of these types of jurisdiction is exclusive. States may often have concurrent jurisdiction and this applies in the cyber realm as well. Note one of the illustrations from the Manual—"a criminal who is a national of State A, but located in State B, may conduct a cyber operation against a web server in State C in order to steal the bank information of individuals located in State D."[67] In that instance, each state would have the ability to exercise jurisdiction.[68] Of course, such a scenario emphasizes the need for international cooperation.

The chapter on jurisdiction concludes with a rule on immunity[69] and a rule about international cooperation.[70] This chapter, while identify-

63. *Id.* at 69–70, ¶ 13.

64. *Id.*

65. *Id.* at 53, ¶ 10–11.

66. *Id.* at 53–54, ¶¶ 10–14.

67. *Id.* at 54, ¶ 15.

68. *Id.*

69. TALLINN MANUAL 2.0 Rule 12 provides that "A State may not exercise enforcement or judicial jurisdiction in relation to persons engaged in cyber activities or cyber infrastructure that enjoy immunity under international law." *Id.* at 71 r. 12.

70. TALLINN MANUAL 2.0 Rule 13 provides that "Although as a general matter States are not obliged to cooperate in the investigation and prosecution of cyber crime, such cooperation

ing some areas where there is no international consensus on an issue or where international law is as yet unclear, is unlikely to cause much controversy.

D. *Law of International Responsibility*

Because of the nature of current cyber activities, this is an extremely important chapter in the Manual. It applies the doctrine of state responsibility, codified mainly in the International Law Commission's Articles on State Responsibility,[71] to cyber actors and cyber activities. There was complete agreement among the Experts that the customary law of state responsibility applies to cyber activities.[72] Rule 14, therefore states that "[a] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation."[73] Neither physical damage nor injury is required for a cyber act to be an internationally wrongful act,[74] and geography is not determinative in determining state responsibility.[75]

The concept of attribution for cyber acts has generated a great deal of discussion and consternation.[76] Rules 15 through 17 address this issue with respect to cyber operations. Rule 15 echoes Articles 4 and 5 of the Articles of State Responsibility and notes that the cyber actions of state organs, such as the CIA or NSA in the United States, are attributable to the state,[77] even if outside that organization's approved authority, or *ultra vires*.[78] For this purpose, organs of the state would also include actors that are not organs by law, but that have "complete dependence" on the state,[79] and persons or entities that are empow-

---

may be required by the terms of an applicable treaty or other international law obligation." *Id.* at 75 r. 13.

71. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001) [hereinafter ILC Draft Articles on Responsibility].

72. TALLINN MANUAL 2.0, *supra* note 14, at 80, ¶ 4.

73. *Id.* at 84 r. 14.

74. *Id.* at 86, ¶ 8.

75. *Id.* at 87, ¶ 11.

76. *See* Lily Hay Newman, *Hacker Lexicon: What is the Attribution Problem?*, WIRED (Dec. 24, 2016, 7:00 AM) https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/; Dimitar Kostadinov, The Attribution Problem in Cyber Attacks, INFOSEC INST. (Feb. 1, 2013), http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref; Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SECURITY L. 229 (2012).

77. TALLINN MANUAL 2.0, *supra* note 14, at 87–90, ¶¶ 3, 8–11.

78. *Id.* at 89, ¶ 9.

79. *Id.* at 88, ¶ 4 (internal citation omitted).

ered to exercise elements of governmental authority.[80]

Even though these statements reflect international law in non-cyber situations, their application to cyber activities is not without controversy. For example, the Experts noted that traditionally the use of government assets such as tanks or warships was a near irrefutable indication of attribution of an activity to a state. The same cannot be said of cyber activities. Indeed, given the ability to capture or spoof cyber infrastructure, including where the cyber activities might originate from, "the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure, or that malware used against hacked cyber infrastructure is designed to 'report back' to another State's governmental cyber infrastructure, is usually insufficient evidence for attributing the operation to that State."[81]

In the case where an organ of the state is put at the disposal of another state, if that organ functions exclusively under the control of the receiving state and takes actions for the purposes and on behalf of that that state, the organ's acts are attributable to the receiving state.[82]

The most difficult legal question in the area of attribution comes from non-state actors who may be working as proxies for a state or who are in some way acting on behalf of a state without clear legal authority to do so. This is addressed by Rule 17,[83] and reflects Article 8 of the Rules of State Responsibility.[84] Many of the discussions around recent cyber events have revolved around the attempt to attribute the actions of private actors to states with whom those actors were aligned.[85] In accordance with international law, cyber operations conducted by non-state actors, but carried out under the "effective control" of a state, are attributable to the state.[86] Mere encouragement or support for the

---

80. *Id.* at 89, ¶¶ 6–9.

81. *Id.* at 91, ¶ 13 (internal citation omitted).

82. *Id.* at 93, ¶ 1.

83. TALLINN MANUAL 2.0 Rule 17 states: "Cyber operations conducted by a non-State actor are attributable to a State when:

(a) engaged in pursuant to its instructions or under its direction or control; or

(b) the State acknowledges and adopts the operations as its own."

Id. at 94 r. 17.

84. ILC Draft Articles on Responsibility, *supra* note 72, art. 8.

85. *See* Dorothy Denning, *The Rise of Hacktivism*, GEO. J. INT'L AFFAIRS (Sep. 8, 2015), http://journal.georgetown.edu/the-rise-of-hacktivism/; Sarah Geary, *The Cyber-Intelligence Nexus: Russia's Use of Proxies*, CIPHER BRIEF (Feb. 24, 2017), https://www.thecipherbrief.com/article/tech/cyber-intelligence-nexus-russias-use-proxies-1092.

86. TALLINN MANUAL 2.0, *supra* note 14, at 95–96, 4–6.

actions of the non-state actor are insufficient to reach attribution.[87] In contrast to the actions of state organs, *ultra vires* acts of non-state actors in these situations are not attributable to the state as they would be acts outside the "effective control" of the state.[88] Finally, if a state does not effectively control a non-state actor, but subsequently adopts the cyber actions of that non-state actor as its own, those acts are also attributable to the state.[89]

As with attribution more generally, it is much easier to identify and state the rule than it is to apply it in factual situations. For example, as noted by the Experts, "a State's preponderant or decisive participation in the 'financing, organizing, training, supplying, and equipping . . . , the selection of its military or paramilitary targets, and the planning of the whole of its operation' has been found insufficient to reach the 'effective control' threshold."[90] In the cyber realm, that might be translated as a state providing the cyber tools, identifying the targets, and selecting the date for the cyber operation to take place and it would still not implicate state responsibility. Some allege this is exactly the scenario with Russia and Russian hacktivists who cyber-assaulted Estonia in the wake of the movement of a Russian war memorial.[91]

Over time, it will be interesting to see how states continue to respond to the high threshold for attribution. As states continue to be the victims of cyber activities that are unattributable to a state, and the rules of sovereignty and due diligence don't allow victim states to require effective action by the host state, the pressure on the attribution standard will increase as a method of allowing victim states to have broader access to countermeasures (discussed below).

Rule 18 covers the doctrines of aiding and assisting, and responsibility for the acts of other states.[92] With respect to aid and assistance, it is

87. *Id.* at 97, ¶ 8.

88. *Id.* at 98, ¶ 13.

89. *Id.* at 99–100, ¶ 17.

90. *Id.* at 97, ¶ 9.

91. R. Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, *in* PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY, PLYMOUTH, 2008, at 163 (2008), https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html.

92. TALLINN MANUAL 2.0 Rule 18 provides that "With respect to cyber operations, a State is responsible for:

> (a) its aid or assistance to another State in the commission of an internationally wrongful act when the State provides the aid or assistance knowing of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it;

vital that the state know that it is actually providing aid and assistance to the internationally wrongful act, and that the state intends to do so.[93] It is also important to note that the aiding state is only responsible for aiding and assisting, not the actual wrongful act.[94] Though not directly dealt with by the Experts, it seems clear that aiding and assisting would require more than allowing transit of harmful data through its cyber infrastructure, even if it did so knowingly. It would defy logic that the standard to trigger the due diligence requirement would be similar or even less than that of the standard of aiding and assisting.

The Manual argues that all the normal circumstances precluding wrongfulness apply to cyber activities.[95] The Manual then embarks on a fairly lengthy discussion of countermeasures.[96] Because countermeasures must not rise to the level of a use of force, cyber activities seem to fit the paradigm well.[97] It is important to note that countermeasures are only available against states and will not preclude the wrongfulness of an act if targeted against non-state actors, unless their actions are attributable to a state.[98] However, the cyber countermeasure need not target the specific organ of the state that is violating international law as the state itself is the target.[99] Additionally, cyber countermeasures are not limited to "in-kind" response. In other words, a state can respond to a non-cyber violation with a cyber countermeasure, and to a cyber violation with a non-cyber countermeasure.[100]

(b) the internationally wrongful act of another State it directs and controls if the State does so with knowledge of the circumstances of the internationally wrongful act and the act would be internationally wrongful if committed by it; or

(c) an internationally wrongful act it coerces another State to commit."

TALLINN MANUAL 2.0, *supra* note 14, at 100 r. 18.

93. *Id.* at 101, ¶ 3.

94. *Id.* at 102, ¶ 6.

95. *Id.* at 104–11. TALLINN MANUAL 2.0 Rule 19 provides that "The wrongfulness of an act involving cyber operations is precluded in the case of:

(a) consent; (b) self-defence; (c) countermeasures; (d) necessity; (e) force majeure; or (f) distress."

Id. at 104 r. 19.

96. *Id.* at 111–34.

97. *See generally* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 718–719 (2014).

98. TALLINN MANUAL 2.0, *supra* note 14, at 113, ¶¶ 7–8.

99. *Id.* at 112–13, ¶ 6.

100. *Id.* at 128–129, ¶ 7.

Cyber countermeasures raise several interesting issues. One of the requirements of a countermeasure is that it be temporary in nature and reversible as far as possible.[101] The Experts understood that requirement broadly and argued in the context of cyber that the deletion of data, even if it prevented some later, post-countermeasure activity, would not bar the countermeasure.[102] The Experts were unable to agree on whether, given two cyber countermeasure options, there was a requirement to utilize the one that was most reversible.[103]

Another element of countermeasures that the Experts found particularly noteworthy is the requirement to notify and potentially seek to negotiate resolution prior to taking a countermeasure.[104] The Experts noted that this requirement was not absolute and agreed that if notifying the target state prior to taking the cyber countermeasure would render the countermeasure ineffective, notification need not be provided.[105] Given the nature of cyber operations, this is a pragmatic approach.

The Experts agreed that cyber countermeasures cannot violate a peremptory norm[106] and must be proportionate to the injury to which they respond,[107] though there is no requirement that the cyber countermeasure target the exact state organ violating international law.[108]

The Experts split on the issue of collective countermeasures with the majority arguing it was not lawful for a non-injured state to take countermeasures on behalf of an injured state.[109] However, the majority then split on the issue of whether a non-injured state may assist the injured state in taking countermeasures.[110]

The remainder of the chapter in the Manual contains rules and commentary on the effect of countermeasures on third parties,[111] the

---

101. ILC Draft Articles on Responsibility, *supra* note 72, art. 49.

102. TALLINN MANUAL 2.0, *supra* note 14, at 119, ¶ 8.

103. *Id.*, ¶ 9.

104. ILC Draft Articles on Responsibility, *supra* note 72, art. 52.

105. TALLINN MANUAL 2.0, *supra* note 14, at 120, ¶ 11.

106. TALLINN MANUAL 2.0 Rule 22 provides that "Countermeasures, whether cyber in nature or not, may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate a peremptory norm. A State taking countermeasures must fulfil its obligations with respect to diplomatic and consular inviolability." *Id.* at 122–23 r. 22.

107. TALLINN MANUAL 2.0 Rule 23 provides that "Countermeasures, whether cyber in nature or not, must be proportionate to the injury to which they respond." *Id.* at 127 r. 23.

108. *Id.* at 129, ¶ 10.

109. *See id.* at 131, ¶ 5.

110. *Id.* at 132, ¶ 7.

111. TALLINN MANUAL 2.0 Rule 23 provides that "A countermeasure, whether cyber in nature or not, that violates a legal obligation owed to a third State or other party is prohibited." *Id.* at 133 r. 23.

plea of necessity,[112] several rules on the obligations of states for internationally wrongful acts,[113] and a rule on the responsibility of international organizations.[114]

These rules and commentary on countermeasures highlight the difference between applying a countermeasure, particularly in cyberspace, as opposed to taking an action in self-defense. The rules and constraints on countermeasures detailed above act as a greater constraint on a state's ability to act in response to actions that do not amount to use of force than actions in response to an armed attack. Importantly, the standards for applying countermeasures are much less discretionary in that certain actual steps must be taken as opposed to a discretionary decision by a state that an action amounts to an armed attack or that an armed attack is imminent. With respect to cyber, this is a particularly important point because so much of the unfriendly cyber interaction between states does not amount to an armed attack.

Perhaps this imbalance is exactly what states desire with respect to cyber countermeasures. This Author has argued elsewhere that easing the ability to use countermeasures may lead to unintended harmful consequences.[115] Nevertheless, it will be interesting to see if in the future, states evolve international law to either lessen the constraints on cyber countermeasures or soften the threshold of an armed attack in order to provide more effective response measures to a greater variety of cyber activities.

E. *Cyber Operations Not Per Se Regulated*

This section of the Manual recognizes that some actions by states are not specifically regulated by international law, but finds a narrow set of actions that fall into this category. As mentioned above with respect to sovereignty,[116] there is a view that this category of unregulated cyber activities is broader. However, the Tallinn Experts took a strict reading of cyber operations not regulated *per se* by international law.

---

112. TALLINN MANUAL 2.0 Rule 23 provides that "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it." *Id.* at 135 r. 23.

113. TALLINN MANUAL 2.0 Rule 27 concerns cessation, assurances, and guarantees; Rules 28 and 29 deal with reparations; and Rule 30 is about *erga omnes* obligations. *See id.* at 142–53.

114. *Id.* at 157 r. 157; *see also id.* at 153–67.

115. *See generally* Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?*, TEX. L. REV. (forthcoming) (on file with the authors).

116. *See supra* Section III.A.

Rule 32 applies to peacetime cyber espionage and takes an almost apologetic tone. Without actually stating that cyber espionage is permitted by international law, the Rule says "[a]lthough peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so."[117] For the purposes of the rule, cyber espionage is defined as "any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information."[118] The rule only applies to espionage conducted by states,[119] and the Experts recognized that not only do many states make espionage illegal as a matter of domestic law when carried out against them,[120] but also that there are a number of states that have specifically authorized certain forms of espionage against other states.[121]

Despite the agreement that even though there is no prohibition *per se*, the Experts agreed that "espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful."[122] However, the Experts could not reach a consensus as to whether remote cyber espionage violated international law. The majority believed that the exfiltration of data violated no rule of international law,. Conversely, a few of the experts believed that at some point the exfiltration might be so severe as to make it illegal.[123] Similarly, the Experts did not agree on close-access operations, such as operations where an individual in the territory of the target state inserts a USB drive into a government system and exfiltrates data. None of the Experts argued that the exfiltration was a violation of international law, but a majority believed it was violative of the target state's sovereignty.[124] The remainder of the Experts viewed espionage as an exception to sovereignty.[125]

The Experts agreed that "honeypots"—valuable data or network segments designed to lure in malicious hackers in order to identify them and examine their methods, but not actually reveal any useful data—were not illegal as a matter of international law.[126] Weaponized

117. TALLINN MANUAL 2.0, *supra* note 14, at 168 r. 32.
118. *Id.*, ¶ 2.
119. *Id.*, ¶ 3.
120. *Id.* at 174, ¶ 17.
121. *Id.* at 169, ¶ 5 (internal citation omitted).
122. *Id.* at 170, ¶ 6.
123. *Id.* at 170–171, ¶ 8.
124. *Id.*
125. *Id.* at 171, ¶ 9.
126. *Id.* at 173–74, ¶ 15.

honeypots, where the data designed to be exfiltrated contains malware that is then executed on the infiltrator's own system, caused a division among the Experts, with the majority finding them completely permissible.[127]

The treatment of espionage in the Tallinn Manual is tied closely to the view of sovereignty. In many of the cases presented where the "method" of espionage might make it illegal, the Experts determined the rule violated was that of sovereignty. Evidence seems to be mounting that cyber-capable nations are engaging in cyber espionage.[128] Increasing cyber espionage is likely to put pressure on the current understanding of how sovereignty applies to the domain of cyberspace, perhaps affecting Rule 32 in the future.

The other rule in this section of unregulated cyber operations says "[i]nternational law regulates cyber operations by non-State actors only in limited cases."[129] With the exception of international law regimes specifically applicable to individuals such as human rights law and the law of armed conflict, the Experts believed that international law did not regulate non-state actors.[130] This is left to be regulated by states through domestic law.

As with espionage, this is an area of international law where the rule is likely to come under pressure. The combination of the volume of incidents caused by non-state actors,[131] the restrictive application of the due diligence rule to states,[132] and the proscription of the use of countermeasures against non-state actors[133] may force states to reconsider the effectiveness of international law with respect to enforcement measures against non-state actors.

---

127. *Id.* at 174, ¶ 16.

128. Kevin Rawlinson, *NSA Surveillance: Merkel's Phone May Have Been Monitored 'for Over 10 Years,'* THE GUARDIAN (Oct. 26, 2013, 15:19 EDT), https://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution; *Russia Behind Hack on German Parliament*, DW.COM (Dec. 11, 2016) http://www.dw.com/en/russia-behind-hack-on-german-parliament-paper-reports/a-36729079; Jose Pagliery, *China Hacked the FDIC–and US Officials Covered it Up, Report Says*, CNN TECH (July 13, 2016, 3:31 PM), http://money.cnn.com/2016/07/13/technology/china-fdic-hack/.

129. TALLINN MANUAL 2.0, *supra* note 14, at 174 r. 33.

130. *Id.* at 175, ¶ 4.

131. Mark Pomerlau, *State vs. Non-State Hackers: Different Tactics, Equal Threat?*, DEF. SYS. (Aug. 17, 2015), https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx.

132. *See supra* Section III.B.

133. *See supra* Section III.D.

F. *International Human Rights Law*

This part of the Manual and those that follow in this Article are separated into what the Experts refer to as Specialized Regimes. These regimes are specialized in that they have developed over time to become their own, somewhat self-contained regimes that govern a narrow range of activities. The Manual applies those regimes to cyber activities.

The first specialized regime covered in the Manual is international human rights law. Many of the difficulties in crafting this portion of the Manual can be directly tied to the lack of clarity with respect to international human rights law more generally.[134] Combined with the vagaries of cyber operations, this chapter contains perhaps the most disagreement among the Experts. Along these lines, one of the important points made with respect to the application of human rights law to cyber operations is that "although a State's activity may interfere with a specific international human right, such as the right to privacy, this fact does not answer the question of whether that right has been violated."[135] In other words, the determination that human rights apply to a cyber activity does not mean that the cyber activity has violated human rights. The potential violation is a separate and additional analysis.

Rule 34 states the general rule of applicability. It says "[i]nternational human rights law is applicable to cyber-related activities."[136] In defining the applicability, the Experts agreed, "as a general principle, customary international human rights law applies in the cyber context beyond a State's territory in situations in which that State exercises 'power or effective control', as it does offline."[137] However, the Experts were split on whether "power or effective control" required "physical" control, with the majority believing physical control was required.[138] The Experts were also split on whether a human rights treaty that was silent on its extraterritorial application should be interpreted as applying extraterritorially. The majority believed that it should be applied extraterritorially in the absence of some provision that limited its

134. TALLINN MANUAL 2.0, *supra* note 14, at 179–82, ¶¶ 1–7. The TALLINN MANUAL 2.0 notes that "the International Group of Experts acknowledged that State understandings concerning the precise scope of certain human rights entitlements in the cyber context, as well as those of human rights tribunals and other relevant human rights bodies, vary." *Id.* at 182, ¶ 1.

135. *Id.* at 181, ¶ 7.

136. *Id.* at 182 r. 134.

137. *Id.* at 184, ¶ 6.

138. *Id.* at 185, ¶ 8.

scope.[139]

Rule 35 states that "Individuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy."[140] This includes the freedom of expression, though the experts could not agree on the precise parameters of that right.[141] The right to hold an opinion[142] and the right to privacy are also protected.[143]

With respect to the right to privacy, the Experts believed that this right "encompasses the confidentiality of communications."[144] The Experts agreed that this protected an individual's private communications from human inspection, but were divided on how the right applied to cases of algorithmic inspections by machines.[145] However, the majority believed that such an inspection did not implicate the individual's right unless and until the state accessed the communications in some way, including data processing.[146] Of course, information available to the public generally does not implicate the right to privacy, even if collected through cyber means, while those available to only a small group could. The Experts were unclear on where these lines actually are drawn between these two situations.[147] The Experts could not agree on how the expectation of privacy applied generally to this right.[148]

The Experts agreed that the right to privacy also protected individuals' "personal data," though the Experts acknowledged that this term is not well defined in international law.[149] With respect to metadata, the Experts agreed that metadata would be considered "personal data" and therefore protected for the purposes of this rule at the point where it was "linked to an individual and relates to that individual's private life."[150] With respect to other metadata, the Experts could not reach a consensus.[151]

---

139. *Id.* at 186, ¶ 11.
140. *Id.* at 187 r. 35.
141. *Id.* at 187–88, ¶¶ 2–4.
142. *Id.* at 188–89, ¶ 5.
143. *Id.* at 189, ¶ 6.
144. *Id.*, ¶ 7 (internal citations omitted).
145. *Id.* at 190, ¶ 8.
146. *Id.*, ¶ 9 n. 420.
147. *Id.* at 190–91, ¶ 10.
148. *Id.* at 191, ¶ 11.
149. *Id.* at 191–92, ¶ 12.
150. *Id.* at 192, ¶ 13.
151. *Id.*, ¶ 14.

The Experts further noted that the customary nature of economic, social, and cultural rights remains unsettled in international law, but agreed that to the extent that they are recognized as rights, cyber operations could certainly implicate those rights.[152] Finally, the Experts noted the claim that there is an international human right of access to the internet and a "right to be forgotten." None of the Experts acknowledged these as rights under current customary law.[153]

Rule 36 states that "[w]ith respect to cyber activities, a State must: (a) respect the international human rights of individuals; and (b) protect the human rights of individuals from abuse by third parties."[154] The obligation to respect human rights applies generally to those rights discussed in the previous rule and applies extraterritorially to applicable rights.[155]

The obligation to protect, or ensure respect for human rights is an affirmative obligation on states, though the Experts acknowledged that some states do not agree that such a rule exists and that the parameters of the rule are at least contested.[156] However, the Experts agreed that such a rule exists, despite its lack of clear definition.[157] For example, the Experts could not agree on the "precise territorial circumstances in which a State has an obligation to protect a particular individual's human rights from interference by third parties."[158]

The Experts agreed that this right included the requirement to take preventive measures such as preventing terrorist impacts on human rights.[159] Relating back to the Experts opinion that there is no right to the internet discussed above, the Experts divided on the issue in which access to the internet was necessary to exercise a human right such as voting.[160] However, the majority of Experts believed that states have no customary right to provide remedies when violations of individual human rights occur.[161]

Rule 37 discusses limitations on the obligation to respect and protect and states "[t]he obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to

152. *Id.* at 194, ¶ 18.
153. *Id.* at 195–96. ¶ 23.
154. *Id.* at 196 r. 36.
155. *Id.*, ¶ 2.
156. *Id.* at 197–98, ¶ 5 (internal citations omitted).
157. *Id.* at 198, ¶ 6.
158. *Id.*
159. *Id.* at 199, ¶ 9.
160. *Id.* at 199–200, ¶ 10.
161. *Id.* at 200, ¶ 12.

certain limitations that are necessary to achieve a legitimate purpose, non-discriminatory, and authorized by law."[162] This rule acknowledges that States must strike a balance concerning cyber activities between individual rights and other important responsibilities, such as public order and national security,[163] though some rights such as protection from slavery and torture are absolute in nature and cannot be limited.[164] The Manual illustrates this point by stating "it is generally considered necessary to restrict the online freedom of expression or right to privacy in order to eliminate child pornography and child exploitation, protect intellectual property rights, and stop incitement to genocide."[165]

In exercising limitations on human rights, the Experts divided on the applicability of the principle of proportionality, with the majority arguing that it did apply.[166] All the Experts believed that whatever limitations were imposed, they must be done non-discriminatorily.[167]

In addition to limitations, states may also derogate from certain human rights obligations, as discussed in Rule 38.[168] This rule is centered completely on treaty law and depends entirely on the specific provisions of the treaty under consideration.

The amount of disagreement among the Experts in this chapter reflects not only the cyber application to human rights law, but the general acceptance of human rights law across states. The Experts noted in many instances that states simply diverge in their views, sometimes dramatically, on the application to human rights law. This is reflected in the application of cyber operations to human rights law. As greater clarity emerges with respect to the primary rules of human rights law, the application to cyber activities will undoubtedly also become clearer.

G. *Diplomatic and Consular Law*

The Chapter on Diplomatic and Consular Law draws heavily from the 1961 Vienna Convention on Diplomatic Relations and the 1963

162. *Id.* at 201–02 r. 37.

163. *Id.* at 202, ¶ 1 (internal citation omitted).

164. *Id.* at 202–03, ¶ 4.

165. *Id.* at 203 (parentheticals and citations omitted).

166. *Id.* at 205, ¶ 9.

167. *Id.* at 206, ¶ 11 (internal citations omitted).

168. TALLINN MANUAL 2.0 Rule 38 states "A State may derogate from its human rights treaty obligations concerning cyber activities when permitted, and under the conditions established, by the treaty in question." *Id.* at 207 r. 38.

Vienna Convention on Consular Relations as substantially reflective of customary international law.[169] The first rule reflects one of the foundational principles of diplomatic and consular law, the inviolability of premises.[170] Though all the Experts agreed with the rule, the application of the rule caused some divided opinions.

The majority believed this protection precluded remote cyber operations on infrastructure located in the premises,[171] as well as diplomatic or consular equipment not located on the premises but used for diplomatic or consular purposes.[172] The Experts were evenly divided on the question of whether third states have an obligation to respect the inviolability of premises or whether that obligation only lies on the host state.[173]

Consideration of Rule 39 prompted discussion of virtual embassies and online diplomatic presences. The Experts did not believe the inviolability extended to these virtual presences, except to the extent that being hosted on the premises as discussed above protected them.[174]

Rule 40 requires that "[a] receiving State must take all appropriate steps to protect cyber infrastructure on the premises of a sending State's diplomatic mission or consular post against intrusion or damage."[175] The application of this rule is dependent on "the magnitude of the threat to the premises, the extent to which the receiving State is aware of a specific threat, and the capacity of the receiving State to take action in the circumstances."[176]

Rule 41 applies the protection given to diplomatic and consular archives, documents, and official correspondence to electronic versions of the same.[177] The Experts were split, however, with respect to private submissions to a mission or consular post, with the majority believing they were covered by extension of the rule.[178] As with premises, the Experts were split with respect to the obligation of third

169. *Id.* at 209, ¶ 1.

170. TALLINN MANUAL 2.0 Rule 39 states "Cyber infrastructure on the premises of a diplomatic mission or consular post is protected by the inviolability of that mission or post." *Id.* at 212 r. 39.

171. *Id.* at 213–14, ¶¶ 5–6.

172. *Id.* at 215–16, ¶¶ 10–12.

173. *Id.* at 214, ¶ 6.

174. *Id.* at 216–17, ¶ 15.

175. *Id.* at 217 r. 40.

176. *Id.* at 217–18, ¶ 2.

177. TALLINN MANUAL 2.0 Rule 41 states "Archives, documents, and official correspondence of a diplomatic mission or consular post that are in electronic form are inviolable." *Id.* at 219 r. 41.

178. *Id.* at 220, ¶ 4.

states to diplomatic or consular archives, documents, and correspondence, with the majority again extending the protections.[179] The Experts were also split on whether the protection continued to apply to communications other than those between the mission and the sending state, such as between the mission and third states. The majority believed that all such communications were protected.[180] Finally, the question was raised concerning normally protected communications that have been disclosed by third parties. In this case, the majority believed that the protection no longer applied.[181]

Rule 42 concerns the right to freedom of communication and states that "[a] receiving State must permit and protect the free cyber communication of a diplomatic mission or consular post for all official purposes."[182] The Experts agreed that receiving states "may not interfere with access to a diplomatic mission's or consular post's website that is used to convey essential information to its citizens in the country, interrupt or slow the Internet connection of a diplomatic mission or consular post, or block or interfere with its cell phones or other telecommunications equipment."[183] The "protect" requirement in this rule is similar to the due diligence rule in that there is still no duty to monitor or take proactive measures to prevent, but merely to remediate when the receiving state has knowledge.

Rule 43 deals with the premises and personnel of states and says:

> (a) [t]he premises of a diplomatic mission or consular post may not be used to engage in cyber activities that are incompatible with diplomatic or consular functions,: and (b) Diplomatic agents and consular officials may not engage in cyber activities that interfere in the internal affairs of the receiving State or are incompatible with the laws.[184]

The section then lists some cyber activities that would be permissible under this rule in a cyber context. Importantly, the Experts concluded that conducting cyber espionage would not be allowed.[185] The section concludes with a rule concerning privileges and immunities of diplo-

179. *Id.* at 221–23, ¶¶ 7–10.
180. *Id.* at 224, ¶¶ 14–15.
181. *Id.*, ¶ 14.
182. *Id.* at 225 r. 25.
183. *Id.* at 226, ¶ 3.
184. *Id.* at 227–28 r. 43.
185. *Id.*

matic and consular personnel,[186] and concludes that the same privileges and immunities apply to cyber related activities.[187]

There are obviously a number of unanswered questions with respect to cyber operations and diplomatic and consular law, particularly with respect to communications. Because so many of those communications now occur via cyber modalities, the application of international law to this area is going to be an important area of legal development.

H. *Law of the Sea*

The law of the sea is a specialized regime with a long history and significant recent codification. The Experts agreed that much of the United Nations Convention on the Law of the Sea[188] reflected customary international law and consequently, the Experts relied on it heavily.[189]

Rule 45 states the general principle of applicability and confirms that "[c]yber operations on the high seas may be conducted only for peaceful purposes, except as otherwise provided for under international law."[190] As an example, the Experts concluded that "[o]f particular note in the cyber context are the high seas freedoms of navigation, overflight, and the laying of submarine cables. Based on, for example, the first two freedoms, both aircraft and vessels are entitled to conduct cyber operations over and in the high seas so long as they do not violate applicable international law."[191] With respect to military cyber operations, the Experts "saw no reason to deviate from the general principle that military activities not involving a prohibited use of force are within the scope of high seas freedoms and other internationally lawful uses of the sea, as set forth in Article 87(1) of the Law of the Sea Convention."[192]

The Experts confirmed the "right of visit" with respect to cyber activities[193] but divided on the permissibility of a "virtual visit," meaning

---

186. TALLINN MANUAL 2.0 Rule 44 states "To the extent diplomatic agents and consular officers enjoy immunities form criminal, civil, and administrative jurisdiction, they enjoy the immunities with regard to their cyber activities." *Id.* at 230 r. 44.

187. *Id.* at 231, ¶¶ 1–4.

188. United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3.

189. TALLINN MANUAL 2.0, *supra* note 14, at 232, ¶¶ 1–2.

190. *Id.* at 233 r. 45.

191. *Id.* at 234, ¶ 3 (citations omitted).

192. *Id.*, ¶ 5 (citations omitted).

193. TALLINN MANUAL 2.0 Rule 46 states "A warship or other duly authorized vessel may exercise the right of visit to board a vessel without flag State consent on the high seas or within an exclusive economic zone if it has reasonable grounds for suspecting the vessel is utilizing cyber

using cyber modalities to conduct the visit.[194] The Experts further confirmed the application of the due regard standard to cyber actions taken in the Exclusive Economic Zone (EEZ),[195] though the Experts split on the legality of conducting military operations in the EEZ with the majority arguing they were permissible.[196]

With respect to the territorial sea and the right of innocent passage, the Experts agreed to Rule 48, which states, "[i]n order for a vessel to claim the right of innocent passage through a coastal State's territorial sea, any cyber operations conducted by the vessel must comply with the conditions imposed on that right."[197] The Experts helpfully listed a number of examples of cyber activities that would render the passage non-innocent.[198] The Experts considered the impact on innocent passage of a state vessel from State A in the territorial waters of State B, conducting cyber operations against State C. The majority of Experts determined this would not be compatible with innocent passage.[199]

Despite the Manual reserving most rules concerning international armed conflict to later in the Manual, Rule 49 says "[d]uring an international armed conflict, a neutral coastal State may not discriminate between the belligerents with respect to cyber operations in that State's territorial sea."[200] Rule 50 returns to more general rules and deals with enforcement jurisdiction in the territorial sea.[201] The Experts divided on the scale of the potential consequences necessary to trigger the right of enforcement jurisdiction. The majority argued that any violation was sufficient, but the minority thought *de minimis* effects

---

means to engage in piracy, slave trading, or unauthorized broadcasting; appears to be without nationality; or is of the nationality of the visiting vessel." *Id.* at 235.

194. *Id.* at 238, ¶ 10.

195. TALLINN MANUAL 2.0 Rule 47 states "In the exercise of its rights and duties, a State conducting cyber operations in the exclusive economic zone of another State must have due regard to that State's rights and duties in the zone and the cyber operations must be conducted for peaceful purposes, except as otherwise provided for under international law." *Id.* at 239.

196. *Id.* at 240, ¶ 4.

197. *Id.* at 241 r. 48.

198. *Id.* at 242–43, ¶ 6–7.

199. *Id.* at 243, ¶ 8

200. *Id.* at 245. r. 49.

201. TALLINN MANUAL 2.0 Rule 50 states "A coastal State may exercise enforcement jurisdiction on-board vessels in the territorial sea with respect to criminal activities involving cyber operations if: the consequences of the crime extend to the coastal State; the crime is of a kind to disturb the public order and security of the coastal State or the good order of the territorial sea; the master of the vessel or the flag State has requested the assistance of the coastal State's authorities; or as necessary to counter drug trafficking." *Id.* at 246 r. 50.

would not trigger the right.[202]

The Experts argued that the standard provisions of the law of the sea apply to cyber operations in the contiguous zone,[203] international straits,[204] archipelagic waters,[205] and to submarine cables.[206] With respect to submarine cables, the Experts could not agree on the application of jurisdiction "between the coastal State and the State laying the submarine communication cable on the coastal State's continental shelf or in its EEZ."[207] Though the Experts agreed that it was violative of international law to damage submarine communication cables, they also agreed that such cables can be tapped to collect and transmit data.[208]

The Manual itself points out areas where the law of the sea is unsettled with respect to cyber operations, such as the need for states to find a method to criminalize willful or negligent damage to submarine communication cables under the high seas.[209] Given the vast amount of data that passes through submarine communication cables, and the increasing ability of states to access them, this is almost certainly an area where state practice will continue to develop.

I. *Air Law*

As with the law of the sea, the Experts determined that international law was generally reflected in the provisions of the most prominent treaty in the area[210]—in this case the 1944 Convention on International Civil Aviation (ICAO), or "Chicago Convention" as it has come to be known.[211] Indeed the terms used throughout the section are governed

202. *Id.* at 247, ¶ 4.

203. TALLINN MANUAL 2.0 Rule 51 states "With respect to vessels located in a coastal State's contiguous zone, that State may use cyber means to prevent or address violations within its territory or territorial sea of its fiscal, immigration, sanitary, or customs laws, including violations perpetrated by cyber means." *Id.* at 248.

204. TALLINN MANUAL 2.0 Rule 52 states "Cyber operations in a strait used for international navigation must be consistent with the right of transit passage." *Id.* at 249.

205. TALLINN MANUAL 2.0 Rule 53 states "Cyber operations in archipelagic waters must be consistent with the legal regime applicable therein." *Id.* at 251.

206. TALLINN MANUAL 2.0 Rule 54 states "The rules and principles of international law applicable to submarine cables apply to submarine communication cables." *Id.* at 252.

207. *Id.* at 255, ¶ 9.

208. *Id.* at 257, ¶ 17.

209. *Id.* at 258, ¶ 19 (internal citations omitted).

210. *Id.* at 259–60, ¶¶ 4–6.

211. The International Civil Aviation Organization Convention on International Civil Aviation, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295.

by definitions in the ICAO.[212]

Rule 55[213] states the rule of general applicability of airspace law to cyber operations on aircraft in national airspace. The Experts noted that this specialized regime only governs the aircraft, and not the cyber operations it is engaged in. Those operations would be governed by other laws, such as those of the subjacent state.[214] With respect to military aircraft—those most likely to be involved in airborne cyber operations—the Experts noted that the Convention requires the permission of the subjacent state for overflight, and allows the subjacent state the right to set the conditions of that overflight, conditions which might include a proscription on cyber operations.[215]

The Experts divided on how to characterize a violation of a state's airspace by another state's military aircraft that is engaged in cyber operations. A minority believed the combination of unconsented presence and the conduct of cyber operations was enough to be an armed attack and trigger the right of self-defense. The majority thought the characterization depended on the nature of the cyber operation. Some of the Experts were also of the view that the mere unconsented presence of a military aircraft authorized the use of force to expel the aircraft from the state's territory.[216]

As opposed to national airspace, cyber operations in international airspace are generally allowed. Rule 56 says "[s]ubject to restrictions thereon contained in international law, a State may conduct cyber operations in international airspace."[217] States may not claim sovereignty over international airspace. Moreover, when conducting cyber operations in international air space, states are only limited by international law proscriptions such as the prohibition on intervention and the use of force, or accepted navigation regimes such as flying over international straits.[218] Additionally, when flying subject to a navigation regime that requires transport in normal mode, the majority of Experts deemed that this did not include active cyber operations, even for aircraft whose purpose is to conduct offensive cyber operations.[219]

---

212. TALLINN MANUAL 2.0, *supra* note 14, at 260.

213. TALLINN MANUAL 2.0 Rule 55 says "A State may regulate the operation of aircraft, including those conducting cyber operations, in its national airspace." *Id.* at 261.

214. *Id.* at 263, ¶ 6.

215. *Id.* at 264.

216. *Id.* at 264–65, ¶¶ 12–13.

217. *Id.* at 265 r. 56.

218. *Id.* at 266, ¶ 4.

219. *Id.* at 266–67, ¶ 5.

Finally, states are precluded from conducting any cyber operations that might jeopardize the safety of the international aviation.[220]

As mentioned earlier, at least with respect to sovereignty,[221] state practice has not taken as restrictive a view toward cyberspace as it has toward airspace. Increasing state capabilities to conduct cyber operations from platforms in the air will potentially result in a clash of paradigms, with the less restrictive cyberspace paradigm giving way to the more restrictive airspace rules. When contrasted with the more liberal space regime discussed below, this difference in legal regulation may push cyber development, particularly with respect to the principle of sovereignty, to space rather than air assets.

J. *Space Law*

Though the spatial differentiation between the law governing airspace and space is not precisely defined,[222] the differences between the two regimes are quite distinct, particularly with respect to the exercise of sovereign authority. The Experts drew a distinction between space-enabled cyber operations, to which space law has only limited application, and cyber-enabled space operations.[223] In drafting the rules, the Experts noted that the applicable treaty law is less complete and less recognized as codifying customary law. However, in the cases where the Experts relied on the language of various space treaties, they did so using provisions they believed were considered customary.[224]

Rule 58 notes the difference in legal proscriptions on the use of cyber on the moon and other celestial bodies and in space more generally. The rule states "(a) [c]yber operations on the moon and other celestial bodies may be conducted only for peaceful purposes. (b) Cyber operations in outer space are subject to international law limitations on the use of force."[225] The Experts concluded as a result of this rule that offensive cyber capabilities could not be placed on the moon, whereas no similar prohibition exists for outer space more generally.[226] With respect to space more generally, the proscription is on the use of cyber capabilities and is governed by the same standards

---

220. TALLINN MANUAL 2.0 Rule 57 says "A State may not conduct cyber operations that jeopardize the safety of international civil aviation." *Id.* at 268.

221. *See supra* Section III.A.

222. TALLINN MANUAL 2.0, *supra* note 14, at 259–60, ¶¶ 1–11; *see also id.* at 271, ¶¶ 3–4.

223. *Id.* at 270–71, ¶¶ 2–3.

224. *Id.* at 272, ¶ 6.

225. *Id.* at 273 r. 58.

226. *Id.* at 273–75, ¶¶ 1–7.

as on earth, including the U.N. Charter.[227]

Rule 59 says "(a) [a] State must respect the right of States of registry to exercise jurisdiction and control over space objects appearing on their registries. (b) A State must conduct its cyber operations involving outer space with due regard for the need to avoid interference with the peaceful space activities of other States."[228]

In accord with this rule, the Experts agreed that states have jurisdiction over their satellites and other space objects and persons thereon, but also noted that this jurisdiction might not be exclusive. For example, if the activities of one state's space objects affect another state's space objects, those states may share concurrent jurisdiction.[229] The Experts also noted that the term "due regard" in this rule carried the same meaning as it does in the law of the sea context.[230]

Finally, respecting the responsibilities of states for cyber activities in outer space, Rule 60 says "(a) [a] State must authorize and supervise the cyber 'activities in outer space' of its non-governmental entities. (b) Cyber operations involving space objects are subject to the responsibility and liability regime of space law."[231]

As more and more private entities begin to operate in outer space, including placing persons in space,[232] this rule will increase in importance. The rule follows treaty law in describing the governance regime as "national" in nature.[233] States must accept responsibility to monitor and approve the actions of non-government entities.

Accordingly, states are generally responsible for their actions under the space law regime which incorporates some of the principles from the Articles of State Responsibility.[234] For example, launching states are liable for damage caused to another state based on a space launch.[235] However, damage caused to space objects by other space objects is based on "fault".[236] The Experts determined these principles apply to

227. *Id.* at 275–77, ¶¶ 8–11.

228. *Id.* at 277, ¶ 4.

229. *Id.* at 278, ¶ 6 n. 229.

230. *Id.* at 279, ¶ 6.

231. *Id.* at 279–80 r. 60.

232. Calla Cofield, *SpaceX to Fly Passengers On a Private Trip Around the Moon in 2018*, SPACE.COM (Feb. 27, 2017, 6:53 PM), http://www.space.com/35844-elon-musk-spacex-announcement-today.html.

233. TALLINN MANUAL 2.0, *supra* note 14, at 280, ¶ 1 (internal citation and quotation marks omitted).

234. *Id.* at 281, ¶ 4 n. 700.

235. *Id.* at 281–82, ¶ 7.

236. *Id.* at 282, ¶ 8.

cyber operations in space as well.

The continued expansion into space will include the increased employment of cyber capabilities. The law surrounding the space regime was formulated when few states had access to space and is fairly permissive, particularly when compared to the rules governing airspace.[237] As more states, including private entities within those states, begin to conduct operations including cyber operations in outer space, the permissive regime may give way to a more limiting regime. At least one major transnational effort is underway now to look more closely at the legal regime applicable to space[238] and it will undoubtedly provide extremely useful input on this important subject.

K. *International Telecommunications Law*

Unlike prior sections of the Manual, which relied primarily on customary international law to support the rules contained therein, in this section of the Manual the Experts note the lack of customary law and explicitly base the following rules on the treaty regime of the International Telecommunications Union.[239] The Experts felt comfortable doing so because "nearly all States are Parties to the treaty regime."[240]

Rule 61 states that "[a] State must take measures to ensure the establishment of international telecommunication infrastructure that is required for rapid and uninterrupted international telecommunications. If, in complying with this requirement, the State establishes cyber infrastructure for international telecommunications, it must maintain and safeguard that infrastructure."[241] The treaty regime establishes three distinct obligations for member states: "to ensure the establishment of infrastructure that facilitates rapid and uninterrupted international telecommunications; to safeguard that infrastructure; and to maintain it."[242] The Experts noted that these are obligations of conduct, not of result, and therefore based on feasibility.[243] Thus, a state need not fulfill its obligation through cyber means, but if it decides to

---

237. U.S. DEP'T OF DEFENSE, OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 2 (2d ed.1999).

238. *See Manual on International Law Applicable to Military Uses of Outer Space*, MCGILL UNIVERSITY, http://www.mcgill.ca/milamos/ (last visited June 4, 2017).

239. TALLINN MANUAL 2.0, *supra* note 14, at 284, ¶ 2.

240. *Id.*

241. *Id.* at 288 r. 61.

242. *Id.*, ¶ 2.

243. *Id.* at 289–90, ¶ 3.

do so, it must safeguard and maintain that cyber infrastructure.[244] As this obligation is a state obligation, the majority of Experts believed it was not lawful for one state to establish communications in another state without the second state's consent.[245]

The Experts determined that states may generally exercise their sovereign authority to suspend or stop communications. Rule 62 says:

> (a) [a] State may suspend, either in part or in full, international cyber communication services within its territory. Immediate notice of such suspension must be provided to other States. (b) A State may stop the transmission of a private cyber communication that appears contrary to its national laws, public order, or decency, or that is dangerous to national security.[246]

However, the Experts note in the commentary that "[t]his right is without prejudice to any international law obligations the State concerned may shoulder prohibiting it from doing so in a particular case"[247] such as diplomatic communications.[248] Assuming communications are suspended, the Experts divided as to the lawfulness of another state restoring communications without the consent of the territorial state. The majority agreed that such action would not be lawful without the consent of the territorial state.[249]

With respect to specific communications, the Experts agreed that stopping specific private cyber communications could include "an instant message, email, or a Tweet."[250]

Rule 63 says "[a] State's use of radio stations may not harmfully interfere with other States' protected use of radio frequencies for wireless cyber communications or services."[251] The Experts accepted the definition of harmful interference to mean interference which "endangers the functioning of a radio navigation service or . . . or seriously degrades, obstructs or repeatedly interrupts a radio communication service operating in accordance with the [International Telecom-

244. *See id.*
245. *Id.* at 290–91, ¶¶ 9–10.
246. *Id.* at 291 r. 62(a)–(b).
247. *Id.* at 291–92, ¶ 1.
248. *Id.* at 294, ¶ 9.
249. *Id.* at 293–94, ¶ 6.
250. *Id.* at 294, ¶ 7.
251. *Id.* r. 63.

munication Union] Radio Regulations."[252] They further agreed that the rule "applies exclusively to interference caused by one State with another's use of frequencies that enable cyber communications or services, wherever those communications or services take place, including in outer space."[253]

Finally, Rule 64 exempts military radio stations and says "[a] State retains its entire freedom under international telecommunication law with regard to military radio installations."[254] Though the rule is limited to radio installations, the Experts agreed that it also included "devices that enable the wireless transmission of data over radio waves."[255] The Experts specified that the exemption only applies to truly "military" installations and not other radio installations put to use by the military in a dual military and civilian capacity.[256]

Though this regime is almost completely treaty-based and not, therefore, viewed as binding customary international law, the practice of inter-state telecommunications will build norms and practices that will undoubtedly help formulate rules with respect to cyberspace. For example, the interaction of a state's right to stop or suspend telecommunications under this regime with emerging human rights expectations concerning individual internet access will continue to refine what state's accept as their legal obligations with respect to cyberspace in the future.

L. *Peaceful Settlement of Disputes*

This section marks the beginning of the transition of the Manual to "International Peace and Security and Cyber Activities." The first three Rules of this section act as a lead-in to the rules on the use of force (*just ad bellum*) and the rules governing armed conflict (*jus in bello*). Because the first three rules are not dealt with in Tallinn 1.0, they deserve some comment here.

Rule 65 concerns states' obligation to peacefully settle their disputes and is based on UN Charter paragraphs 2(3) and 33(1)[257] and is

252. *Id.* at 296, ¶ 7 n. 728 (internal citations omitted).

253. *Id.* at 296–97, ¶ 8.

254. *Id.* at 298 r. 64.

255. *Id.* at 299, ¶ 2.

256. *Id.*, ¶ 4 (internal citation omitted).

257. U.N. Charter, art. 2(3) states: "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered." Art. 33(1) states: "The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by

generally accepted as customary international law.[258] The Rule states: "(a) States must attempt to settle their international disputes involving cyber activities that endanger international peace and security by peaceful means; (b) If States attempt to settle international disputes involving cyber activities that do not endanger international peace and security, they must do so by peaceful means."[259]

The Experts agreed that this rule only applies to international disputes and "not to purely internal ones."[260] However, the Experts disagreed on the application to a transnational dispute between a state and a non-state actor with only a minority believing such conflicts were covered.[261] Despite this disagreement, the Experts agreed that "peaceful means," when required, did not limit a resort to lawful means such as countermeasures or the use of force in self-defense, or any measure authorized by the United Nations Security Council.[262]

States must exercise good faith in attempting to peacefully settle their cyber disputes,[263] but need neither be successful, nor exhaust all possible peaceful means in order to comply with this obligation.[264] The Experts also agreed that this obligation continues even in times of hostilities if peaceful means remain open as to a specific cyber dispute.[265] The Experts further agreed that states must still use peaceful means if they endeavor to solve international disputes that do not endanger international peace and security, but that states are under no obligation to attempt to solve international disputes if they choose not to do so.[266]

Given the increasing number of international and transnational cyber disputes, this rule is extremely important. Recent cyber disputes between states[267] and between states and non-state

---

negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice."

258. *See* TALLINN MANUAL 2.0, *supra* note 14, at 303, ¶ 1.

259. *Id.* at 304.

260. *Id.* at 304, ¶ 2.

261. *Id.* at 305, ¶ 6-7.

262. *Id.* at 307, ¶ 11, 13.

263. *Id.* at 308, ¶ 14.

264. *Id.* at 309, ¶ 17-18.

265. *Id.* at 309-10, ¶ 20-21.

266. *Id.* at 310, ¶ 22-23.

267. *See* Gina Chon, *U.S. Pursues Case Against Chinese Army Hackers*, FINANCIAL TIMES (Sept. 24, 2015), https://www.ft.com/content/a378b4c6-62b0-11e5-9846-de406ccb37f2 (discussing the U.S. indictment of five Chinese military members for cyber theft); Jane Perez, *Xi Jingping Pledges to Work With U.S. to Stop Cybercrimes*, N.Y. TIMES (Sept. 22, 2015) https://www.nytimes.com/2015/09/23/

actors[268] have generally been resolved by peaceful means, but as the severity of the cyber interventions increases, this rule will likely be tested. Russian President Putin's seemingly dismissive acknowledgement of "patriotic" Russians intervening in U.S. elections,[269] discussed in the next section, highlights the importance of clarity in applying principles of sovereignty,[270] due diligence,[271] and the remedies of retorsion and countermeasures[272] to cyber activities. The more effective various "peaceful means" prove to be at resolving cyber disputes, the more content states will be to rely on them.

M. *Prohibition of Intervention*

The customary prohibition on intervention is divided into two rules in the Manual, the first dealing with States and the second with the United Nations.

Rule 66 states the well-recognized international law principle:[273] "A State may not intervene, including by cyber means, in the internal or external affairs of another State."[274] The rule only applies to relations

world/asia/xi-jinping-of-china-to-address-wary-us-business-leaders.html?_r=0 (explaining the agreement between China and the United States to work together to stop cyber crime by China in the United States.); David Lee, *Russia and Ukraine in cyber 'stand-off'*, BBC (Mar. 5, 2014), http://www.bbc.com/news/technology-26447200 (discussing the recent exchange of cyber hacks between Ukraine and alleged Russian state cyber forces).

268. *See* Alastair Stevenson, *It Looks Like the US Government Just Got Hacked Again—and This Time Anonymous is Claiming Responsibility*, BUS. INSIDER (July 24, 2015, 7:45 AM) http://www.businessinsider.com/anonymous-hackers-leak-4200-us-government-workers-alleged-details-to-protest-ttip-and-tpp-2015-7 (discussing Anonymous's hack of the United States Census Bureau); Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.adaf6a618dbe; *Anonymous 'Hacks' North Korea Social Media Accounts*, BBC (Apr. 4, 2013), http://www.bbc.com/news/technology-22025724 (discussing Anonymous's hacking of social media accounts in North Korea).

269. Ian Phillips & Vladimir Isachenkov, Putin: Russia Doesn't Hack but "Patriotic" Individuals Might, U.S. News & World Rep. (June 1, 2017), https://www.usnews.com/news/world/articles/2017-06-01/putin-russian-state-has-never-been-involved-in-hacking (discussing President Putin's claims that Russia does not hack as a state function, but that patriotic Russians may decide to on their own).

270. *See supra* Part IIIA.

271. *See supra* Part IIIB.

272. *See supra* Part IIID.

273. *See* TALLINN MANUAL 2.0, *supra* note 14, at 312, 314, ¶ 1, 5.

274. *Id.* at 312.

between states,[275] and only proscribes coercive interference.[276] Though the Experts felt the "precise contours and application of the prohibition of intervention are unclear in light of ever-evolving and increasingly intertwined international relations,"[277] they concurred in the definition provided by the International Court of Justice that a prohibited intervention must bear on a state's *domaine réservé*, meaning such matters are the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[278]

The Experts also agreed that "the scope of *domaine réservé* may shrink as States commit issues related to cyberspace to international law regulation,"[279] but concluded that the "matter most clearly within a State's *domaine réservé* appears to be the choice of both the political system and its organization."[280] With respect to coercion, the Experts split on whether the coercion must be "designed to infuence outcomes in, or conduct with respect to, a matter reserved to a target State," with the majority agreeing that it did.[281] They also split on whether the coercive act had to directly cause the effect, with the majority arguing it did not, "so long as there is a causal nexus."[282]

Similarly, the Experts did not agree on whether the state had to actually know it was being coerced for the intervening state to be violating international law. The majority decided such knowledge was not a necessary precondition.[283] On the other hand, the Experts agreed that knoweldge that the cyber coercion was coming from a state (or an entity attribuatable to a state) was not required for a violation,[284] though intent to coerce was required.[285] Further, the effectiveness of the coercion was immaterial as to whether there was an intervention.[286]

The Experts split on whether cyber operations designed to protect its nationals that were in the target state would amount to internvention,

275. *Id.* at 313, ¶ 4.

276. *Id.* at 313, ¶ 3.

277. *Id.* at 314, ¶ 6.

278. *Id.* at 315, ¶ 8 (quoting Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 205 (June 27).

279. *Id.* at 316, ¶ 13.

280. *Id.* at 315, ¶ 10.

281. *Id.* at 318, ¶ 19.

282. *Id.* at 320, ¶ 24.

283. *Id.* at 320, ¶ 25.

284. *Id.* at 321, ¶ 26.

285. *Id.* at 321, ¶ 27.

286. *Id.* at 322, ¶ 29.

with the majority deciding that they generally would not.[287] Though the Experts agreed that economic measures, such as unilateral economic sanctions, would not amount to an intervention,[288] they were split concerning cyber operations in support of humanitarian intervention in the absence of a United Nations Security Council authorization, with the Experts divided along the lines of whether they believed humanitarian intervention itself was lawful.[289]

Rule 67 continues the discussion of intervention but focuses on actions by the United Nations. The rule states "The United Nations may not intervene, including by cyber means, in matters that are essentially within the domestic jurisdiction of a State. This principle does not prejudice the taking of enforcement measures decided upon by the UN Security Council under Chapter VII of the United Nations Charter."[290] A few Experts believed this rule should apply to international organizations generally, but consensus could only be achieved on applying it to the United Nations.[291]

The basis of this rule is Article 2(7) of the United Nations Charter which prohibts the United Nations from intervening in "matters which are essentially within the domestic jurisdiction of any state."[292] As a result, the Experts agreed that this rule would not limit actions concerning international peace and security.[293] While the Experts agreed that the matters that fell in the scope of article 2(7) has been constricting,[294] they agreed that despite the rule being phrased in terms of intervention, for matters truly within the domestic jurisdiction of any state, even non-coercive interference by the United Nations would violate this rule.[295]

The prohibition on cyber intervention has become very important in light of recent allegations of Russian cyber intervention into elections

287. *Id.* at 323, ¶ 34.
288. *Id.* at 324, ¶ 35.
289. *Id.* at 324, ¶ 36.
290. *Id.* at 325.
291. *Id.* at 325, ¶ 1.
292. UN Charter, art. 2, ¶ 7.
293. *See* TALLINN MANUAL 2.0, *supra* note 14, at 325, ¶ 2.
294. *Id.* at 326, ¶ 4.
295. *Id.* at 326, ¶ 5.

in both the United States[296] and Europe.[297] While no target of Russian hacking has yet declared such activities to be a violation of international law, President Obama did make a somewhat veiled threat to President Putin in October 2016 over the famous "red phone," by telling President Putin that "[i]nternational law, including the law of armed conflict, applies to actions in cyber space."[298]

The tepid internatioinal response to what has long been understood as the stereotype of a prohibited intervention may be pushing the boundaries of previously recognized norms. The Manual's strong statement will hopefully be one clear articulation of the prohibition as applied to cyber activities that states can begin to use to push back against Russian cyber operations.

Of course, as long as President Putin can simply attribute the cyber meddling to "patriotic hackers," and then accept no responsibility to control them or limit their activities,[299] international law will have little impact on cyber intervention. This, once again, highlights the importance of the future evolution of the due diligence principle and its potential to more strictly impose responsibility on states for the cyber actions of those within their borders or under their control.

The remainder of the Manual provides rules with respect to the *jus ad bellum* and the *jus in bello*, and is only slightly amended from the rules as published in the Tallinn Manual 1.0.[300] Therefore, no highlights will be provided here.

IV. Conclusion

It is important to remember that the Experts who participated in the Tallinn Manuals were committed to stating the law as it was and to producing Manuals that would be understood to be their own views

296. David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. Times (Dec. 9, 2016), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics&region=rank&module=package&version=highlights&contentPlacement=4&pgtype=collection.

297. Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA Today (Jan. 9, 2017, 7:03 AM), https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/.

298. William M. Arkin, Ken Dilanian & Cynthia McFadden, *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC News (Dec. 19, 2016, 6:30 PM), http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116.

299. *See* Phillips and Isachenkov, *supra* note 270.

300. *See* Tallinn Manual 2.0, *supra* note 14, at 328–562; *see also* Tallinn Manual 1.0, *supra* note 13, at 42–256.

and not those of states. The Experts were humbler in their intention for the project than some others who have commented on it. In fact, as noted at the U.S. launch of the Manual by Mr. Rutger van Marrising from the Ministry of Foreign Affairs of the Kingdom of the Netherlands, Tallinn 2.0 is really designed to be the beginning of a longer and more significant discussion.[301]

Nevertheless, Tallinn 2.0 will be the starting point for the discussion for the next several years and perhaps longer. Its comprehensive nature, informed analysis and conclusions, and incorporation of both state and peer comments all make it the most valuable reference and starting point for a discussion on the international law applicable to cyber operations.

As this Article notes, there are still many areas of disagreement and lack of clarity, even amongst the Experts who wrote the Tallinn Manuals. There are also many situations where states have not spoken or acted publically with respect to cyber operations. This is still a growing area of the law and one in which there exists a great need for insight and understanding to create new approaches to existing problems. However, until states clarify exactly where the law is headed, Tallinn 2.0 will serve as the starting point for moving forward with the law on cyber operations.

301. *See* Corn, *supra* note 28.