Cyber Sovereignty: The Way Ahead

ERIC TALBOT JENSEN*

SUMMARY

---

* Associate Professor, Brigham Young University Law School. The author would like to thank the staff of the *Texas International Law Journal* for hosting an excellent symposium and the attendees for their insights and comments to the author's presentation. Additionally, Grant Hodgson and Brooke Robinson provided excellent research and review assistance for this Article.

PREFACE

> There is no universally agreed definition [for sovereignty], but considerations of international sovereignty revolve around the recognition of a government's right to exercise exclusive control over territory, and this definition is ill suited for cyber discussions. For convenience we might refer to "the geography of cyberspace," but I challenge you to point to cyberspace. Although cyberspace is all around us, when trying to point at it you will be as unable to as the Square in [Edwin] Abbott's Flatland was to point to "up." I always found it troubling to hear military commanders talk in terms of seizing the cyber "high ground" or negotiating "cyber terrain." That was language they were comfortable with, but in any meaningful sense of the word, cyber lacks geography.[1]

Recent years are full of reports of cyber incidents in which, from time to time, significant damage is done by way of a cyber operation. Examples include the 2007 cyber assault on Estonia by pro-Russian "hacktivists" that temporarily shut down many governmental and private sector operations,[2] the 2012 "Shamoon" virus that damaged 30,000 computers at Saudi Arabia's Aramco and was claimed by the "Cutting Sword of Justice,"[3] the 2013 cyber shutdown of the New York Times by the Syrian Electronic Army,[4] and of course the infamous Stuxnet malware that damaged almost one thousand centrifuges at an Iranian nuclear facility and has been attributed to the United States and Israel by many cyber experts.[5]

---

1. Gary D. Brown, *The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214, 225–26 (2013). Gary Brown was the first Staff Judge Advocate (legal advisor) for the newly formed United States Cyber Command. *Id.* at 214.

2. Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, EUR. INST. (2008), http://www.europeaninstitute.org/index.php/component/content/article/42-european-affairs/winterspring-2008/67-cyber-war-i-estonia-attacked-from-russia (discussing the cyber attacks on Estonia and Estonia's defensive response).

3. *Saudi Arabia Says Cyber Attack Aimed to Disrupt Oil, Gas Flow*, REUTERS (Dec. 9, 2012, 2:30 PM), http://www.reuters.com/article/2012/12/09/saudi-attack-idUSL5E8N91UE20121209; *see also* Wael Mahdi, *Saudi Arabia Says Aramco Cyberattack Came from Foreign States*, BLOOMBERG (Dec. 9, 2012), http://www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html.

4. Heather Kelly, *Syrian Group Cited as* New York Times *Outage Continues*, CNN (Aug. 29, 2013, 9:30 AM), http://www.cnn.com/2013/08/27/tech/web/new-york-times-website-attack/ (discussing the attack that temporarily shut down the *New York Times*' website).

5. Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST, June 2, 2012, http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Each of these cyber events, and the multitude of others that have occurred and continue to occur daily,[6] raises important questions about the role and responsibility of States with respect to cyber incidents. Do States exercise sovereign control over the cyber infrastructure that sits on their territory? If so, do States have a responsibility to control the cyber activities that emanate from or even just pass through their sovereign cyber assets? In other words, to what extent does a State have to control activities of non-State actors, such as private hacktivists, criminal organizations, and terrorists, when those cyber actions may cause harm to others?

The answer to these questions revolves in large part around the international law doctrine of sovereignty.[7] The extent to which nations exercise sovereignty over cyberspace and cyber infrastructure will provide key answers to how much control States must exercise and how much responsibility States must accept for harmful cyber activities when they fail to adequately do so.

This Article argues that States have sovereign power over their cyber infrastructure and that with that sovereign power comes corresponding responsibility to control that infrastructure and prevent it from being knowingly used to harm other States. This responsibility to prevent external harm extends not

---

6. *See generally* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 (Jason Healey ed., 2013).

7. The continuing application of international law to cyber capabilities has led one scholar to conclude:

> This does not necessarily mean that the rules and principles of international law are applicable to cyberspace in their traditional interpretation. Because of the novel character of cyberspace, and in view of the vulnerability of cyber infrastructure, there is a noticeable uncertainty among governments and legal scholars as to whether the traditional rules and principles are sufficient to provide answers to some worrisome questions.

Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 127 (2013). China, Russia, Tajikistan, and Uzbekistan seem to believe that new treaties governing cyber conflict are needed. *See* Permanent Representatives of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations, Letter dated 12 Sept. 2011 to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14, 2011) ("China, Russia, Tajikistan and Uzbekistan have jointly elaborated in the form of a potential General Assembly resolution on an international code of conduct for information security and call for international deliberations within the United Nations framework on such an international code, with the aim of achieving the earliest possible consensus on international norms and rules guiding the behaviour of States in the information space." (citation omitted)); Wu Jiao & Zhao Shengnan, *Nations Call on UN to Discuss Cyber Security*, CHINA DAILY, Sept. 14, 2011, http://europe.chinadaily.com.cn/europe/2011-09/14/content_13682694.htm (discussing letter from China, Russia, Tajikistan, and Uzbekistan to United Nations calling for new rules for cyber conflict); Jason Healey, *Breakthrough or Just Broken? China and Russia's UNGA Proposal on Cyber Norms*, ATLANTIC COUNCIL (Sept. 21, 2011), http://www.atlanticcouncil.org/blogs/new-atlanticist/breakthrough-or-just-broken-china-and-russia-s-unga-proposal-on-cyber-norms [hereinafter Healey, *Breakthrough or Just Broken?*] (same). However, other countries, including the United Kingdom and the United States, have advocated that current international law is insufficient to govern cyber war. *See, e.g.*, U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General: Addendum*, at 4, U.N. Doc. A/59/116/Add.1 (Dec. 28, 2004) (discussing the United States' acknowledgment of the need for international cooperation to assure cybersecurity); U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, at 11–12, U.N. Doc. A/59/116 (June 23, 2004) (asserting the United Kingdom's position that the Council of Europe Convention on Cybercrime is the best means for criminalizing cybercrime).

only to State actors, but also to non-State actors. This sovereign power and responsibility, while almost exclusive, necessarily has some limitation.

The Introduction to this Article will introduce the underlying assumptions of sovereignty and set the stage for a review of some of the cardinal principles of sovereignty and their application to cyberspace in light of each State's corresponding sovereign duties and obligations. Parts I and II will then look at the fundamental principles of sovereignty, consider how these principles apply to cyber activities and what corresponding cyber duties and obligations those principles implicate, and then consider related issues that naturally arise from that application.

INTRODUCTION

In the emerging area of cyber operations, the application of the doctrine of sovereignty to cyber activities has created an ongoing debate among States,[8] academics,[9] and practitioners.[10] The recently published *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*) reflects some of this controversy in its short section on sovereignty.[11]

Current State practice suggests that States are hesitant to accept responsibility for cyber activities that come from within their sovereign territory.[12] In none of the examples discussed in the Preface did any State accept responsibility for the cyber actions that occurred.[13] In fact, the opposite is true. In the case of the cyber assaults on Estonia, Russia not only disclaimed any responsibility, but has proven unresponsive to requests by Estonia for investigation and extradition of the potential offenders who acted from within Russian territory.[14] In the case of the

8. *See generally* Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., *Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2010), *transmitted by Note of the Secretary-General*, U.N. Doc. A/65/201 (July 30, 2010) [hereinafter Int'l Sec. Grp.] (chronicling States' approaches to cybersecurity); U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, U.N. Doc. A/64/129/Add.1 (Sept. 9, 2009) [hereinafter *Developments in the Field of Information and Telecommunications*] (reporting on how States have responded to the security concerns surrounding new developments in the fields of information and telecommunications).

9. *See, e.g.*, *generally* Forrest Hare, *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*, *in* THE VIRTUAL BATTLEFIELD: PERSPECTIVES ON CYBER WARFARE 88 (Christian Czosseck & Kenneth Geers eds., 2009); Andrew Liaropoulos, *Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?*, *in* PROCEEDINGS OF THE 8TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 136 (Douglas Hart ed., 2013); von Heinegg, *supra* note 7; Sean Kanuck, *Sovereign Discourse on Cyber Conflict under International Law*, 88 TEX. L. REV. 1571, 1597 (2010); Eric Talbot Jensen, *Sovereignty and Neutrality in Cyber Conflict*, 35 FORDHAM INT'L L.J. 815 (2012) [hereinafter Jensen, *Sovereignty and Neutrality*].

10. Brown, *supra* note 1, at 218.

11. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE r. 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL]. The Author was a member of the international group of experts that drafted the Manual.

12. *See* Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 277 (2014) [hereinafter Schmitt, *The Law of Cyber Warfare*] ("[I]t is typically left to potential targeted states to safeguard cyber activities and cyber infrastructure on their territory.").

13. *See supra* notes 2–5 and accompanying text.

14. *See* Ruus, *supra* note 2 (discussing lack of Russian cooperation following the attack).

Stuxnet malware, despite numerous allegations that the United States and Israel were involved, neither country has officially admitted responsibility.[15]

This hesitation on the part of States to accept responsibility for incidents that occur over the Internet is the product of two major issues inherent in the structure of the Internet: the difficulty of timely attributing an attack and the random method in which data travels over the Internet infrastructure, normally taking the path of least resistance without respect to geography.[16]

The issue of cyber attribution has been well documented[17] and needs only brief comment here. The nature of the Internet allows anonymity, including for those who desire to represent themselves to be someone else. This anonymity acts as "an open invitation to those who would like to do [] harm, whatever their motives."[18] This inherent difficulty in timely attribution makes States wary of accepting responsibility for attacks from within their territory because not only can they not always identify the attacker in a timely manner, but because even if they can identify the computer from which the cyber act originates, they are unlikely to know who is behind the computer.[19]

Similarly, anonymity allows States to take actions, knowing that timely attribution is impossible.[20] This is especially true of actions taken by States through proxies, such as non-State actors.[21]

---

15. David E. Sanger, *Obama Order Sped up Wave of Cyberattacks against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all&; *but see* William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all (noting tacit U.S. and Israeli acknowledgment of the Stuxnet virus).

16. *See* David Hricik, *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 466–70 (1998) (outlining the complex process through which information is fragmented and disseminated through the internet according to the best path available, creating a random set of transmission paths at any moment).

17. *See generally* MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR (2009); Jack M. Beard, *Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law*, 47 VAND. J. TRANSNAT'L L. 67 (2014); Susan W. Brenner, *Cyber-Threats and the Limits of Bureaucratic Control*, 14 MINN. J. L. SCI. & TECH. 137 (2013); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 397–401 (2011); Todd C. Huntley, *Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare*, 60 NAVAL L. REV. 1, 34–35 (2010); Erik M. Mudrinich, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, 68 A.F. L. REV. 167 (2012); Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602 (2011); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014); Jonathan Solomon, *Cyberdeterrence between Nation-States: Plausible Strategy or a Pipe Dream?*, 5 STRATEGIC STUD. Q. 1, 5–10 (2011), *available at* http://www.au.af.mil/au/ssq/2011/spring/solomon.pdf.

18. Harry D. Raduege, Jr., *Fighting Weapons of Mass Disruption: Why America Needs a "Cyber Triad"*, *in* GLOBAL CYBER DETERRENCE: VIEWS FROM CHINA, THE U.S., RUSSIA, INDIA, AND NORWAY 3, 4 (Andrew Nagorski ed., 2010), *available at* http://www.ewi.info/sites/default/files/ideas-files/CyberDeterrenceWeb.pdf.

19. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 785–86 (2012).

20. *See id.* (discussing how the difficulty of attributing cyber attacks enables cyber attackers).

21. *See id.* at 781 (emphasizing the ability of non-State actors to carry out attacks and "harness the

Additionally, the nature of data flow on the Internet makes States hesitant to accept responsibility for cyber activities that flow from within their territory. Cyber data, by its nature, seeks out the path of least resistance over the available cyber infrastructure.[22] In other words, an email sent from a computer in one city to a recipient in that same city may travel through any number of foreign countries before arriving at its destination.[23] The same is true of cyber malware. And this data is not only uncontrollable by the sender in how it travels, but also largely uncontrollable by the States through which the data passes. This means that malware may traverse any number of States before reaching the target State. Transit States do not want to be responsible for the harmful data in these types of scenarios.

Despite the hesitance of States to accept responsibility for attacks crossing their cyber infrastructure, there is a fundamental assumption in international law that authority and obligations strive to stay in balance with each other.[24] In other words, when the international paradigm allocates authority to a State, it almost always allocates a corresponding responsibility or obligation.[25] The application of this principle was illustrated as far back in history as the legitimization of the Westphalian system. When States became the primary actors in the international community, they did so with the understanding that they would possess a monopoly on force within their geographic borders.[26] In correspondence to that obligation came the grant of authority for sovereigns to raise armies and navies that would be reciprocally recognized by other States and given combatant immunity in any future conflicts, as long as those armies and navies acted in accordance with the sovereign's wishes and the provisions of any international agreements to which the sovereign had acceded.[27]

The practical application of this balance is seen in the Instruction for the Government of Armies of the United States in the Field,[28] known as the Lieber

---

power of cyber weapons and use them at their discretion" without the threat of retribution).

22. *See* Hricik, *supra* note 16, at 467 (noting that the internet "is based on TCP/IP (Transfer Control Protocol/Internet Protocol) routing of information packets through unpredictable paths through interconnected networks linking millions of computers." (internal quotation marks omitted)).

23. *See id.* at 469 (explaining how an email can "be broken into hundreds or thousands of packets, each potentially traversing several different networks around the globe" before reaching its destination (internal quotation marks omitted)).

24. *See* Martti Koskenniemi, *Doctrines of State Responsibility*, *in* THE LAW OF INTERNATIONAL RESPONSIBILITY 45, 47–48 (Philip Alston & Vaughan Lowe eds., 2010) (discussing the reciprocal nature of authority and obligations in international law).

25. *Id.*

26. W. Michael Reisman, *Sovereignty and Human Rights in Contemporary International Law*, 84 AM. J. INT'L L. 866, 867 (1990); Frédéric Gilles Sourgens, *Positivism, Humanism, and Hegemony: Sovereignty and Security for Our Time*, 25 PENN ST. INT'L L. REV. 433, 443 (2006) (citing sixteenth-century writer Bodin's *Six Livres De la République* as defining sovereignty as the "absolute and perpetual power of the commonwealth resting in the hands of the state"). *See generally* PHILIP BOBBITT, THE SHIELD OF ACHILLES: WAR, PEACE, AND THE COURSE OF HISTORY 81–90, 96–118 (2002) (discussing the development of the concept of sovereign power).

27. *See* Viet D. Dinh, *Nationalism in the Age of Terror*, 56 FLA. L. REV. 867, 871–73 (2004) (discussing key characteristics of the Westphalian system, including the State monopoly on violence); *cf.* BOBBITT, *supra* note 26, at 509–19 (recounting the development of the Westphalian system and Grotius's ideas of sovereignty).

28. U.S. War Department, General Orders No. 100: Instructions for the Government of Armies of the United States in the Field (Apr. 24, 1863) [hereinafter Lieber Code], *available at* http://www.icrc.org

Code.[29] This Code was written by Francis Lieber and issued by President Abraham Lincoln to provide guidance to the Union armies during the American Civil War.[30] Article 57 of the Lieber Code proclaims, "So soon as a man is armed by a sovereign government and takes the soldier's oath of fidelity, he is a belligerent; his killing, wounding, or other warlike acts are not individual crimes or offenses."[31] In other words, once the sovereign was exercising the responsibility to monopolize and control violence through its agents, those agents were granted authority to use force on behalf of the sovereign with immunity, even when fighting against other sovereigns.[32]

This balance between responsibility and authority continues to underlie the modern law of armed conflict. The laws with respect to prisoners of war,[33] the treatment of civilians during armed conflict,[34] and targeting[35] all reflect the balanced grant of authority and obligation. The balance also applies directly to the principle of sovereignty. As stated in the International Court of Justice's (ICJ) *Corfu Channel* case, "Sovereignty confers rights upon States and imposes obligations on them."[36]

As a starting point, it is important to note that international law must also be considered to apply to cyberspace and cyber technologies. As stated in the United States' 2011 International Strategy for Cyberspace, "The development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding State behavior—in times of peace and conflict—also apply in cyberspace."[37]

/ihl.nsf/FULL/110?OpenDocument.

29. *Id.*; *see also* JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY 8 (2012) ("Historians and international lawyers who discuss [Instruction for the Government of Armies of the United States in the Field] usually call the order Lieber's code after its principal drafter.").

30. WITT, *supra* note 29, at 2 ("President Lincoln will issue Lieber's code as an order for the armies of the Union. He will deliver it to the armies of the Confederacy, too, and expect them to follow the rules he has set out. The code will be published in newspapers across the country and distributed to thousands of officers in the Union Army.").

31. Lieber Code, *supra* note 28, art. 57.

32. Eric Talbot Jensen, *Applying a Sovereign Agency Theory of the Law of Armed Conflict*, 12 CHI. J. INT'L L. 685, 708–10 (2012).

33. Geneva Convention Relative to the Treatment of Prisoners of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention on Prisoners of War]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

34. *E.g.*, Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; Additional Protocol I, *supra* note 33.

35. Additional Protocol I, *supra* note 33.

36. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

37. EXEC. OFFICE OF THE PRESIDENT OF THE U.S., INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011) [hereinafter OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

It follows, then, that the international law doctrines applying to sovereignty would apply to cyber technologies. Where international law grants authority for States with respect to cyberspace and the application of cyber technologies, it also imposes duties and obligations. As nations exercise sovereign power over aspects of cyberspace, or exert sovereign authority over cyber infrastructure, they must necessarily accept the corresponding obligations and duties that come with that assertion of authority.

The following Parts of this Article will review some of the cardinal principles of sovereignty and their application to cyberspace and then consider the corresponding duties and obligations. In each case, the principle of sovereignty will be stated and defined. Its application to cyberspace will then be discussed, including the corresponding duty or obligation that arises from that assertion of sovereignty. An example of the duty and obligation will be used to help clarify the analysis. Finally, issues that arise from the assertion of that authority and its corresponding duty or obligation will be highlighted.

I. STATES ARE SOVEREIGN AND EQUAL

When the nation-State emerged in seventeenth-century Europe, it brought with it the doctrine that the international community would consist of geographically organized and controlled entities that would have at least two characteristics. First, those entities would be sovereign, and second, they would be equal, regardless of size or composition.[38] These two characteristics of States remain in force today and have significant impacts on cyberspace and cyber operations.

A. Sovereignty

Sovereignty is inherent to statehood and, in fact, is often termed the "basic constitutional doctrine of the law of nations."[39] The meaning of the term "sovereignty" has been a point of discussion for centuries[40] and remains so today.[41] However, it is manifested in certain rights and corresponding obligations. A basic review of those rights and obligations will assist in discerning the impact of sovereignty on cyber operations.

---

38. *See* BOBBITT, *supra* note 26, at 508 (noting that in the aftermath of the Thirty Years War, "[t]he extension of the maxim *cuius regio eius religio* imposed common restrictions on states, adumbrating the emergence of a new society of states characterized by their sovereign equality").

39. *E.g.*, JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 447 (8th ed. 2012).

40. *E.g.*, SAINT AUGUSTINE, THE CITY OF GOD 88 (Vernon J. Bourke ed., Gerald G. Walsh et al. trans., 1958) (426); JOHN AUSTIN, THE PROVINCE OF JURISPRUDENCE DETERMINED 191–361 (Isaiah Berlin et al. eds., 1954) (1861); THOMAS HOBBES, LEVIATHAN OR THE MATTER, FORME, AND POWER OF A COMMON-WEALTH ECCLESIASTICAL AND CIVILL 121–29 (Richard Tuck ed., 1991) (1651); JOHN LOCKE, TWO TREATISES OF GOVERNMENT 105 (Thomas I. Cook ed., 1947) (1690).

41. *E.g.*, John Alan Cohan, *Sovereignty in a Postsovereign World*, 18 FLA. J. INT'L L. 907, 908–09 (2006); Reisman, *supra* note 26, at 866.

1. Rights

Sovereignty confers rights on two distinct planes or spheres: the domestic sphere and the international sphere. In other words, sovereignty is understood to be "the collection of rights held by a State, first in its capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane, representing that territory and its people."[42]

With respect to the domestic sphere, sovereignty provides exclusivity in power and authority. This was confirmed in the *Island of Palmas* Arbitral Award of 1928.[43] The arbitral decision provides that "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[44] One of the most fundamental rights of sovereignty, then, is exclusivity of power within the sovereign's own territory, particularly as opposed to the exercise of rights in that territory by some other sovereign.[45]

The ICJ in its *Corfu Channel* decision confirmed this understanding of sovereignty. "By sovereingty [sic], we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States."[46]

Though a State's sovereign power is nearly absolute, it is limited by certain international law principles,[47] including actions of the U.N. Security Council,[48] the law of armed conflict,[49] and fundamental human rights.[50] There are also areas where, based on consensual agreement and custom, no State can assert sovereignty, such as the high seas.[51] This area has been treated as *res communis*, meaning that it

---

42. CRAWFORD, *supra* note 39, at 448.

43. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

44. *Id.*

45. Samantha Besson, *Sovereignty, in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 119 (2011). Sovereignty is generally characterized as the "powers and privileges resting on customary law which are independent of the particular consent of another state." CRAWFORD, *supra* note 39, at 448.

46. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

47. Besson, *supra* note 45, para. 75.

48. For example, each member of the United Nations has agreed to "accept and carry out the decisions of the Security Council in accordance with the present Charter." U.N. Charter art. 25.; *see also* John R. Worth, *Globalization and the Myth of Absolute National Sovereignty: Reconsidering the "Un-signing" of the Rome Statute and the Legacy of Senator Bricker*, 79 IND. L.J. 245, 260 (2004) (discussing States' relinquishment of some powers in accepting the legitimacy and authority of the United Nations).

49. For example, during times of international armed conflicts, States have to treat prisoners of war in accordance with the Geneva Conventions, rather than any potentially applicable domestic law. *See generally* Geneva Convention on Prisoners of War, *supra* note 33.

50. *See* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 684–85 (2004) (outlining that "core rights . . . cannot be eliminated"); Ashley S. Deeks, *Consent to the Use of Force and International Law Supremacy*, 54 HARV. INT'L L.J. 1, 11 (2013) (noting that international human rights laws "trump inconsistent domestic laws").

51. Allison Leigh Richmond, *Scrutinizing the Shipwreck Salvage Standard: Should a Salvor Be Rewarded for Locating Historic Treasure?*, 23 N.Y. INT'L L. REV. 109, 121 (2010).

belongs to all States and can be appropriated by no State.[52] There are other areas where actors have agreed to non-exclusive sovereignty such as Antarctica,[53] the seabed,[54] and the moon.[55] These are areas where no sovereign exercises power, but where all sovereigns share power, based on agreement.

2. Obligations

As discussed above, international law tries to keep in balance rights and obligations. This is reflected in the ICJ's statement, "Sovereignty confers rights upon States and imposes obligations on them."[56] Therefore, in correspondence with the rights and authorities discussed above, the principle of sovereignty also imposes obligations which deserve discussion here.

Obligations tied to sovereignty include the obligation to recognize the sovereignty of other States,[57] the obligation of non-intervention into the areas of exclusive jurisdiction of another State,[58] and the obligation to control the actions that occur within the sovereign's geographic boundaries.[59]

The obligation to recognize the sovereignty of other States is simply the obverse of the right of a State to exercise its own sovereignty. In claiming the rights that come with sovereignty, there is an implicit recognition of the right of others to make similar claims and exercise similar rights.

Once another State has made such claims, and those claims are recognized, other sovereigns have a legal obligation to not interfere with the sovereign rights of the other State. Though there are legitimate exceptions to this rule,[60] the obligation of non-intervention is well recognized in international law.[61]

---

52. Jean Allain, *Maritime Wrecks: Where the* Lex Ferenda *of Underwater Cultural Heritage Collides with the* Lex Lata *of the Law of the Sea Convention*, 38 VA. J. INT'L L. 747, 758 (1998).

53. *See* The Antarctic Treaty art. 4, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71 (limiting claims to sovereignty in Antarctica).

54. U.N. Convention on the Law of the Sea arts. 1, 137, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397.

55. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies art 2, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

56. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 43 (Apr. 9) (individual opinion of Judge Alvarez).

57. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 289 (7th ed. 2008) ("The sovereignty and equality of states represent the basic constitutional doctrine of the law of nations...."); Michael J. Kelly, *Pulling at the Threads of Westphalia: "Involuntary Sovereignty Waiver"—Revolutionary International Legal Theory or Return to Rule by the Great Powers?*, 10 UCLA J. INT'L L. & FOREIGN AFF. 361, 364 (2005) ("Under classic Westphalian theory, the base maxim upon which foreign relations are built is the proposition that all states are equal and must reciprocally respect each other's sovereignty.").

58. CRAWFORD, *supra* note 39, at 447 ("The corollaries of the sovereignty and equality of states [include] ... a duty of non-intervention in the area of exclusive jurisdiction of other states ....").

59. Ilaşcu v. Moldova, 2004-VII Eur. Ct. H.R. 1, para. 312 ("[J]urisdiction is presumed to be exercised normally throughout the State's territory.").

60. For example, lawful countermeasures or actions taken in self-defense would allow a nation to interfere with another State's sovereignty. *See* U.N. Charter art. 51 (allowing a right of individual or collective self-defense in the event of an armed attack against a Member State of the United Nations).

61. *E.g.*, *Corfu Channel*, 1949 I.C.J. at 35 ("Between independent States, respect for territorial sovereignty is an essential foundation of international relations.").

Another obligation that grows out of sovereignty is the requirement to control actions from within a State's sovereign control from having deleterious effects on others.[62] This obligation is worth mentioning here but will be discussed further below.

B. Equality

The principle of the sovereign equality of States laid out in Article 2.1 of the U.N. Charter States: "The Organization is based on the principle of the sovereign equality of all its Members."[63] This principle of equality is based on the historical maxim "*par in parem non habet imperium*," or "an equal has no power over an equal,"[64] which is considered by some to be the first, and perhaps most fundamental, principle of sovereignty.[65] As such, certain rights and obligations accrue from this accepted equality.

1. Rights

As equals under international law, States have the right to deal with each other on equal footing, with equal consideration under the law. "If states (and only states) are conceived of as sovereign, then in this respect at least they are equal, and their sovereignty is in a major aspect a relation to other states (and to organizations of states) defined by law."[66] While skeptics argue that the practical reality of this is far from being true, with large and powerful States clearly exerting unequal pressures on smaller and weaker States to bow to their desires,[67] equality is still guaranteed under the law. Regardless of what some identify as the reality of international politics where "while all States are equal, some are more equal than others,"[68] the legal regime is established with a clear preference to equality and maintenance of the status quo. "The United Nations are [sic] based on the principle of sovereign equality of all its members and preserving state sovereignty is a top priority for both international organizations and individual States."[69]

---

62. *See infra* Part I.B.2.

63. U.N. Charter art. 2, para. 1.

64. CRAWFORD, *supra* note 39, at 448 & n.9.

65. U.N. Charter art. 2, para. 1.

66. CRAWFORD, *supra* note 39, at 447.

67. *See, e.g.*, *Philippines Seeks Quick UN Ruling on South China Sea Dispute*, S. CHINA MORNING POST, June 19, 2014, http://www.scmp.com/news/asia/article/1536058/philippines-seeks-quick-un-ruling-south-china-sea-dispute ("China claims most of the South China Sea, including waters near the shores of its neighbours, which has led to escalating territorial disputes."); Russell Hotten & Alix Kroeger, *Ukraine-Russia Gas Row: Red Bills and Red Rags*, BBC (June 16, 2014), http://www.bbc.com/news/world-europe-26987082 (stating that the gas conflict is a "power struggle between the interim Ukrainian government, which leans towards the EU, and Russia, which wants to keep Ukraine firmly within its sphere of influence").

68. CRAWFORD, *supra* note 39, at 449 (citing GEORGE ORWELL, ANIMAL FARM 90 (1945)).

69. Liaropoulos, *supra* note 9, at 137–38 (citation omitted).

Some of the obvious rights that accrue from international equality include an equal right to global commons,[70] the right to develop and utilize domestic resources without non-consensual external constraints,[71] and the right to discourse on the international scene as an equal. These rights are also tempered with corresponding obligations.

2. Obligations

Several obligations flow from the principle of sovereign equality. First, States must act with due regard for the rights of other sovereigns.[72] There is some discussion as to how far-reaching this obligation of due regard is, but it is at least applicable by treaty to the global commons,[73] natural resources,[74] the environment,[75] and during times of armed conflict.[76]

The obligation of due regard, though not clearly defined in international law, is generally thought of as an obligation to ensure that the exercise of one State's rights does not cause undue harm to another State's exercise of its rights.[77] It is

---

70. *See* Todd B. Adams, *Is There a Legal Future for Sustainable Development in Global Warming? Justice, Economics, and Protecting the Environment*, 16 GEO. INT'L ENVTL. L. REV. 77, 97 (2003) ("[The world] is to be shared by all generations in accordance with the limited rights and necessary obligations of a user of the natural resources or the trustee of the natural resources .... '[P]lanetary rights' are group rights to equal access to the commons." citing EDITH BROWN WEISS, IN FAIRNESS TO FUTURE GENERATIONS: INTERNATIONAL LAW, COMMON PATRIMONY, AND INTERGENERATIONAL EQUITY 96 (1989))).

71. *See* Inaamul Haque & Ruxandra Burdescu, *Monterrey Consensus on Financing for Development: Response Sought from International Economic Law*, 27 B.C. INT'L & COMP. L. REV. 219, 249–50 (2004) ("Under customary international law, principles of sovereignty support a state's clear right to regulate commercial activities within its borders. This power is extensive and encompasses such issues as capacity to engage in business, forms of business enterprises, conditions of continuance of a business, and regulations of capital markets as well as those of foreign capital inflows and outflows.").

72. *E.g.*, George K. Walker, *Defining Terms in the 1982 Law of the Sea Convention IV: The Last Round of Definitions Proposed by the International Law Association (American Branch) Law of the Sea Committee*, 36 CAL. W. INT'L L.J. 133, 168–69 (2005) ("Article 87(2) declares that the high seas freedoms listed in Article 87(1) ... 'shall be exercised by all States with due regard of the interests of other States in their exercise of the freedom of the high seas, and also with due regard for the rights under [the] Convention with respect to activities in the Area.'" (alteration in original) (quoting U.N. Convention on the Law of the Sea, *supra* note 54, art. 87(2))).

73. *E.g.*, Outer Space Treaty, *supra* note 55, art. 9; Geneva Convention on the High Seas art. 2, Apr. 29, 1958, 13 U.S.T. 2312, 450 U.N.T.S. 82.

74. G.A. Res. 1803 (XVII), U.N. GAOR, 17th Sess., Supp. No. 17, U.N. Doc. A/5217, at 15 (Dec. 14, 1962); Charles N. Brower & John B. Tepe, Jr., *The Charter of Economic Rights and Duties of States: A Reflection or Rejection of International Law?*, 9 INT'L LAW. 295, 306–07 (1975).

75. *See* Meinhard Schröder, *Precautionary Approach/Principle*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 45, at 4 (describing the precautionary principle as a set of rules guiding States towards environmentally stable development). *See generally* United Nations Conference on Environment and Development, Rio de Janeiro, Braz., June 3–14, 1992, *Report of the United Nations Conference on Environment and Development*, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I) (Aug. 12, 1992).

76. DEP'T OF THE NAVY ET AL., THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS para 8.4 (2007); 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 147–49 (2005); SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA § 35 (Louise Doswald-Beck ed., 1995); U.K. MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT para 12.24 (2004).

77. *See* Chinthaka Mendis, Sovereignty vs. Trans-Boundary Environmental Harm: The Evolving

understood to have two components: 1) an "awareness and consideration of either State interest(s) or other factor(s)," and 2) a balancing of those interests and factors when making a decision.[78]

Another obligation that has its foundation in sovereign equality is the obligation to solve disputes peacefully. This obligation is clearly stated in the U.N. Charter[79] and has been stated in General Assembly statements and resolutions,[80] applied in decisions of the ICJ,[81] and has been duplicated in bilateral and multilateral treaties.[82]

While there is no obligation to solve all disputes, States are obligated to resolve disputes peacefully if they have the potential to endanger the maintenance of international peace or security.[83] Additionally, if States elect to resolve disputes that do not endanger international peace and security, they must also resolve these disputes peacefully, though there is no legal obligation to resolve these disputes at all.[84]

C. Application to Cyberspace

As stated above, the doctrine of sovereignty and the principles it espouses have direct application to cyberspace. As States exercise their sovereign rights, they can do so in cyberspace but must also accept the corresponding obligations that apply. The next two Subparts will consider the principles of sovereignty and equality and apply the rights and obligations discussed above to cyberspace, as well as identify some lingering issues that will need further resolution.

1. Sovereignty

As a matter of sovereignty, States have the right to develop their cyber capabilities according to their own desires and resources. A State may choose to extensively develop its cyber capabilities and make them available broadly to its citizens as Estonia has done,[85] or it can choose to close its cyber borders to outside influences as North Korea has done.[86]

International Law Obligations and the Sethusamuduram Ship Channel Project 54–55 (2006) (unpublished U.N. fellowship manuscript), http://www.un.org/depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/mendis_0607_sri_lanka.pdf (illustrating the obligation of due regard with discussion of Sri Lanka and India).

78. Walker, *supra* note 72, at 174.

79. U.N. Charter art. 2, paras. 3–4; *Id.* arts. 33–38.

80. G.A. Res. 40/9, U.N. Doc. A/RES/40/9 (Nov. 8, 1985); G.A. Res 2625 (XXV), U.N. GAOR, 25th Sess., U.N. Doc. A/8082, at 121 (Oct. 24, 1970).

81. Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21).

82. *See id.* para. 22 (noting claims to resolve disputes peacefully in cited bilateral and multilateral treaties).

83. U.N. Charter art. 33, para. 1.

84. G.A. Res. 2625 (XXV), *supra* note 80.

85. *Cyber Security*, E-ESTONIA.COM, http://e-estonia.com/the-story/digital-society/cyber-security/ (last visited Feb. 7, 2015) ("CERT-EE (Computer Emergency Response Team Estonia) handles security

In conjunction with this right, States are obligated to recognize this right and not interfere with the domestic cyber decisions of another State.[87] For example, except as provided by international law, one State cannot place limits on the ability of another with respect to its cyber development and capabilities.[88] States can, either bilaterally or multilaterally, agree to collaborate on cyber activities or place limits or constraints on such development between or among themselves.[89]

Because of the place of a State on the international sphere, States may express their intent and work toward the development of State practice, either alone or in conjunction with others. In line with this, many States have actively participated in international fora, such as the U.N.-sponsored Group of Government Experts,[90] and regional fora, such as the Shanghai Cooperation Organization[91] or the Council of Europe.[92] As with any international agreement, States have the obligation to negotiate in good faith[93] and to comply with their international obligations, once undertaken.

One of the recently developing pressures on the idea of cyber sovereignty is the movement to recognize a human right to the Internet.[94] If the time comes that

---

incidents taking place in the .ee domain. The department helps in case Estonian websites or services should fall under cyber attack or if Estonian computers distribute malware. CERT-EE also has the possibility to reverse engineer the malware .... [T]he real key to Estonian cyber security lies in the inherent safety and security built-in to every single Estonian e-Government and IT infrastructure system. The secure 2048-bit encryption that powers Estonia's Electronic-ID, digital signatures and X-road-enabled systems means that personal identity and data in Estonia is airtight.").

86. Dave Lee, *North Korea: On the Net in World's Most Secretive Nation*, BBC (Dec. 10, 2012), http://www.bbc.com/news/technology-20445632.

87. *See* TALLINN MANUAL r. 1 (observing that sovereignty gives States the exclusive right to control cyber infrastructure and cyber activities within their boundaries).

88. *See id.* (delineating exclusive rights associated with State sovereignty in cyberspace).

89. *See, e.g.*, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 9 (2011) [hereinafter DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE], *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/DOD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf (describing the Department of Defense's plan to develop "increasingly robust international relationships to reflect [its] core commitments and common interests in cyberspace").

90. Int'l Sec. Grp., *supra* note 8, at 7–8.

91. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 865–66 (2012).

92. Convention on Cybercrime pmbl., Nov. 23, 2001, T.I.A.S No. 13174, E.T.S. No. 185 (2001) [hereinafter Convention on Cybercrime].

93. *See, e.g.*, Aerial Incident of 10 August 1999 (Pak. v. India), Judgment, 2000 I.C.J. 12, para. 53 (June 21) ("The Court's lack of jurisdiction does not relieve States of their obligation to settle their disputes by peaceful means .... They are [ ] under an obligation to seek [a peaceful settlement], and to do so in good faith ...."); G.A. Res. 2625 (XXV), *supra* note 80, at 123 (reaffirming U.N. Charter principles related to peaceful resolution of conflicts); Draft Declaration on Rights and Duties of States, G.A. Res. 375 (IV), annex art. 13, U.N. GAOR, 4th Sess., U.N. Doc. A/1251, at 67 (Dec. 6, 1949) ("Every State has the duty to carry out in good faith its obligations arising from treaties and other sources of international law ...."); Markus Kotzur, *Good Faith (Bona Fide)*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 45, paras. 11–14 (discussing treaties that require good-faith negotiation).

94. *See* Written Statement Submitted by the Association for Progressive Communications (APC), a Non-Governmental Organization in General Consultative Status, U.N. Doc. A/HRC/17/NGO/38 (May 24, 2011) (associating "Internet rights" with human rights). *See also* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, para. 22, U.N. Doc. A/HRC/17/27 (May 16, 2011) ("The right to freedom of opinion and expression is as much

such a human right is recognized and accepted by States, that right will, of course, impose obligations on the sovereign decisions of each State, constraining State action that might affect the enjoyment of that human right by its population.

Additionally, a State's exercise of sovereignty over cyber resources can be directed or limited by the U.N. Security Council through the power granted to it in the U.N. Charter.[95] States have a duty to comply with Security Council resolutions, even if they limit the exercise of sovereignty over cyber issues. Additionally, States must comply with human rights obligations, even if it limits their exercise of sovereignty.[96]

For example, assume State A contracts for the use of cyber capabilities from State C. Assume further that State A is using cyber means to incite human rights abuses in State B through the cyber infrastructure provided by State C. If the Security Council orders State C to stop allowing State A to use its cyber infrastructure, State C must comply.

2. Equality

Just as States are equals under the doctrine of sovereignty, each State exercises its sovereign cyber prerogatives on an equal plane with all others. Each State, regardless of its cyber capabilities, has the same right to exercise sovereignty over its territory as any other State. However, in doing so, conflicts often arise between States.[97] Certain obligations attach to States in these disputes.

First, States have an obligation to resolve peacefully cyber disputes that may endanger international peace and security.[98] If States attempt to resolve cyber disputes that don't endanger international peace and security, they must do so peacefully.[99]

For example, if State A is using cyber means to harm State B, and that action is endangering international peace and security, both States have an obligation to resolve the dispute peacefully. Alternatively, if State A is using cyber means to steal information from State B, but that theft of information does not endanger

---

a fundamental right on its own accord as it is an 'enabler' of other rights . . . ."); Cassondra Mix, *Internet Communication Blackout: Attack Under Non-international Armed Conflict?*, 3 J.L. & CYBER WARFARE 70, 99 (2014) (noting the suggestions that an Internet blackout imposed by Egyptian authorities to quell protests in 2011 may have violated a right to the Internet).

95. U.N. Charter art. 25 ("The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter.").

96. *See, e.g.*, International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, 999 U.N.T.S. 171 (establishing the civil and political rights of all individuals as well as States' obligations to protect those rights).

97. *See, e.g.*, Lesley Wroughton & Michael Martina, *Cyber Spying, Maritime Disputes Loom Large in U.S.-China Talks*, REUTERS (July 8, 2014), http://www.reuters.com/article/2014/07/08/china-usa-idUSL4N0PJ0MT20140708 (noting increased tensions between the United States and China regarding the territorial scope of cyber activities).

98. *See* U.N. Charter art. 2, para. 3 ("All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.").

99. *Id.*

international peace and security, a dispute may arise, but there is no obligation to try to settle that dispute. However, if attempts to settle that dispute are made, those methods must be peaceful.

Second, in its cyber activities, a State must exercise due regard for the rights of other States.[100] For example, assume a State wants to increase its cyber security. In an effort to do so, it decides to aggressively monitor cyber threats across the World Wide Web. That State has the right to do so, so long as its activities do not violate the rights of other sovereign States.

D. The Way Ahead

This principle of sovereign equality raises some lingering issues that continue to be the focus of the international community. Because States are sovereign and equal, each State is able to develop its cyber capabilities based on its own best interest. Further, each State has no obligation to get involved in other States' domestic cyber issues unless it chooses to do so. However, there is a great deal of discussion about cyber collaboration, particularly as it relates to less developed countries.

The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recently stated in its report that "[c]onfronting the challenges of the twenty-first century depends on successful cooperation among like-minded partners. Collaboration among States, and between States, the private sector and civil society, is important and measures to improve information security require broad international cooperation to be effective."[101] This collaboration would "be designed to share best practices, manage incidents, build confidence, reduce risk and enhance transparency and stability."[102]

Information sharing and capacity building claims revolve mostly around calls for "ensuring global [information and communications technology] security,"[103] and many States have responded favorably to some of these ideas.[104] In the Department of Defense's Cyberspace Policy Report, the Department of Defense stated,

> In collaboration with other U.S. Government agencies, Allies and partners, [the Department of Defense] pursues bilateral and

---

100. *See supra* notes 72–78 and accompanying text (discussing the duty of due regard and its broad applicability under international law).

101. Int'l Sec. Grp., *supra* note 8, para. 15.

102. *Id.* para. 14.

103. *E.g.*, *id.* para. 17.

104. *See, e.g.*, *EU–Japan ICT Cooperation–Joining Forces for the Future Internet*, EUR. COMM'N, https://ec.europa.eu/digital-agenda/en/eu-japan-ict-cooperation-%E2%80%93-joining-forces-future-internet (last visited Feb. 8, 2015) (stating that European countries began joint research projects with Japan in 2012 to design efficient, global technology, including internet security technologies, "for the future networked society"); Press Release, White House, FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security (June 17, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol (indicating that the United States and Russian Federation took measures to increase cooperation on information and communications technology security in order to reduce the possibility of a cyber incident destabilizing their bilateral relationship).

> multilateral engagements to develop further norms that increase openness, interoperability, security, and reliability. International cyberspace norms will increase stability and predictability of state conduct in cyberspace, and these norms will enable international action to take any required corrective measures.[105]

The balance that will have to be struck between the exercise of sovereign prerogative with respect to cyber activities and the benefits of information and security sharing for the health of the Internet will continue to be a vexing issue for the foreseeable future. For now, there is no obligation to engage in information and security sharing, but much pressure to do so.

Finally, the equality of States means that each State has an equal vote in the discussion of how to resolve lingering cyber issues. For example, a group of States headed by Russia recently proposed a "code of conduct" for cyber activities.[106] Other nations, such as the United States, did not support such an initiative.[107] States may choose to band together in regional alliances with respect to cyber activities[108] or may take unilateral action.[109] No consensus is required in a system of sovereign equality.

II. STATES EXERCISE SOVEREIGNTY OVER TERRITORY, PERSONS, AND ACTIVITIES

Though sovereignty manifests itself in many different ways, it almost always means that a sovereign has some kind of territory over which it exercises ultimate control.[110] This territorial authority extends to the population and activities within the territory.[111] As clearly stated in one of the seminal treatises on international law, "The corollaries of the sovereignty and equality of states [include] a jurisdiction, prima facie exclusive, over a territory and the permanent population living there . . . ."[112]

---

105. U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT 5–6 (2011) [hereinafter DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT] *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

106. Wu & Zhao, *supra* note 7.

107. Healey, *Breakthrough or Just Broken?*, *supra* note 7.

108. *See* JOHN LYONS, ESTABLISHING THE INTERNATIONAL CYBER SECURITY PROTECTION ALLIANCE IN ASIA PACIFIC (ICSPA APAC) 1 (2014) (announcing the establishment of an alliance in the Asia Pacific to enhance online safety and security and provide governments and law enforcement agencies with resources and expertise to help them reduce harm from cyber crime).

109. Abraham D. Sofaer et al., *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 179 (The Nat'l Acad. Press ed., 2010) ("[C]urrent U.S. efforts to deter cyberattacks and exploitation—though formally advocating international cooperation—are based almost exclusively on unilateral measures.").

110. *See* Besson, *supra* note 45, para. 1 (defining sovereignty as "supreme authority within a territory).

111. *Id.* para. 70 (referring to sovereignty as encompassing "ultimate authority and competence over all people and all things within [the sovereign's] territory").

112. CRAWFORD, *supra* note 39, at 447.

The rest of Part II will discuss the sovereign rights and obligations with respect to territory and persons, and then apply these rights and obligations to cyberspace, including identifying particular issues that remain unsettled.

A. Territory

Sovereignty over a territory denotes certain rights and corresponding obligations associated with that specific territory.

1. Rights

Perhaps the most important sovereign right over territory is the exclusivity of authority. As von Heinegg has stated, "territorial sovereignty protects a State against any form of interference by other States."[113] Sovereigns alone exercise this right and are only encroached upon through consensual divestiture of authority.[114] Even the UN Charter grants States protection under Article 2(7) against intervention from the United Nations, and other States in certain matters, concerning issues that fall within a State's domestic jurisdiction.[115]

Sovereignty over territory necessarily implies sovereignty over things found on or within territory. For example, "[O]bjects owned by a State or used by that State for exclusively non-commercial government purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State if located outside the territory of another State."[116] This exclusivity of jurisdiction would also apply to objects that have sovereign immunity, wherever located.[117] Additionally, objects not owned by the State but located within the State's territory are subject to the State's regulation.[118] This would include both real and personal property.[119]

States also exercise authority to control their geographic borders.[120] This implies that "the State is entitled to control access to and egress from its territory," which "seems to also apply to all forms of communication."[121]

---

113. von Heinegg, *supra* note 7, at 124.

114. *See* Cohan, *supra* note 41, at 935 (explaining how States can willingly enter into agreements that undermine their domestic sovereignty by recognizing external authority structures).

115. U.N. Charter art. 2, para. 7; Besson, *supra* note 45, para. 88 ("The UN Charter also protects sovereign States' domaine réservé and prohibits other States' intervention on sovereign States' territory." (citations omitted)).

116. von Heinegg, *supra* note 7, at 130.

117. TALLINN MANUAL r. 4.

118. von Heinegg, *supra* note 7, at 124.

119. HENRY WHEATON, ELEMENTS OF INTERNATIONAL LAW § 77 (George Grafton Wilson ed., 1936) (1836).

120. Hare, *supra* note 9, at 92.

121. von Heinegg, *supra* note 7, at 124.

2. Obligations

The principle of sovereign equality entails an obligation of all States to respect the territorial sovereignty of other States. As the ICJ noted in the *Nicaragua* judgment, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[122]

Another extremely important obligation that each sovereign State has is to not knowingly allow its territory to be used to harm another State.[123] This obligation is well founded in international law and stated clearly in the ICJ's *Corfu Channel* case where the court says a State may not "allow knowingly its territory to be used for acts contrary to the rights of other States."[124]

Accordingly, States are required under international law to take appropriate steps to protect the rights of other States.[125] This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage or have the potential to inflict such damage on persons and objects protected by the territorial sovereignty of the target State.[126]

These obligations, as applied to cyber operations, generate interesting discussion, as will be covered in further detail below. While it is mostly clear how they apply in the non-cyber world, cyber operations have caused many to rethink the practical application of these foundational sovereign obligations.[127]

B. Persons

The ability of a sovereign State to assert power over persons has been uncontroversial since the genesis of statehood.[128] However, the bounds of that

---

122. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 202 (June 27) (quoting another source).

123. Corfu Channel (U.K. v Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

124. *Id.*

125. *See, e.g.*, United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, paras. 67–68 (May 24) (describing the general obligation under international law for States to "ensure the most constant protection and security to each other's nationals in their respective territories." (internal quotation marks omitted)).

126. In the *Trail Smelter* case, the arbitral tribunal, citing the Federal Court of Switzerland, noted: "This right (sovereignty) excludes . . . not only the usurpation and exercise of sovereign rights . . . but also an actual encroachment which might prejudice the natural use of the territory and the free movement of its inhabitants." Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963 (1941) (first omission and part of second omission in original). According to the tribunal, "under the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes . . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence . . . ." *Id.* at 1965.

127. *See, e.g.*, Eric Talbot Jensen, *State Obligations in Cyber Operations*, 14 BALTIC Y.B. INT'L L. 71 (2014) [hereinafter Jensen, *State Obligations*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2419527 (describing how recent cyber incidents have drawn attention to State obligations to control their cyber infrastructure to ensure it does not harm other States).

128. *See, e.g.*, Cohan, *supra* note 41, at 944 ("[T]he concept of sovereignty . . . has previously been characterized as the right of a State to exercise supreme power over its territory and citizens, free from outside interference."); von Heinegg, *supra* note 7, at 132 ("Moreover, according to the principles of

assertion have often been contested, including in a seminal case decided by the Permanent Court of International Justice (PCIJ), the precursor to the ICJ. In *S.S. "Lotus"*, a dispute arose between France and Turkey over Turkey's assertion of authority in the case of an accidental collision at sea.[129] The Court in that case determined that the public international law regime was fundamentally permissive and that where there was no positive restriction, sovereigns were generally free to assert their authority over individuals in the absence of a specific proscription from doing so.[130]

While that specific decision of the PCIJ has been limited under modern international law,[131] a State's current ability to exercise sovereignty applies to all legal persons within its territory and some outside its territory, such as its citizens who are abroad.[132] This means that a State's sovereign rights and obligations extend to both State and non-State actors who meet those qualifications.

1. Rights

Sovereign States' ability to exercise prescriptive jurisdiction (territorial,[133] nationality,[134] protective,[135] passive personality,[136] and universal[137]) over both State and non-State actors is guided by international law.[138] These accepted limitations represent the modern constraints on the assertion of such jurisdiction.[139] Conflicting

---

active and passive nationality, a State is entitled to exercise its jurisdiction over the conduct of individuals that occurred outside its territory.")

129. S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 5 (Sept. 7).

130. *Id.* at 18 ("International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.").

131. *See* U.N. Convention on the Law of the Sea, *supra* note 54, art. 97 ("In the event of a collision or any other incident of navigation concerning a ship on the high seas, involving the penal or disciplinary responsibility of the master or of any other person in the service of the ship, no penal or disciplinary proceedings may be instituted against such person except before the judicial or administrative authorities either of the flag State or of the State of which such person is a national.").

132. *See* Helen Stacy, *Relational Sovereignty*, 55 STAN. L. REV. 2029, 2050–51 (2003) ("Sovereignty attaches itself to the people of the state, not merely the state itself.... Relational sovereignty places a higher obligation on the sovereign state to care for and regulate the behavior of its citizens both inside and outside state borders.").

133. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(1) (1986).

134. *Id.* § 402(2).

135. *Id.* § 402(3) & cmt. f.

136. *Id.* § 402 & cmt. g.

137. *Id.* § 404.

138. *See* INT'L BAR ASS'N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11 (2009) ("The starting point for jurisdiction is that all states have competence over events occurring and persons (whether nationals, residents or otherwise) present in their territory.... In addition, states have long recognised the right of a state to exercise jurisdiction over persons or events located outside its territory in certain circumstances, based on the effects doctrine, the nationality or personality principle, the protective principle or the universality principle.").

139. *See id.* at 11–16 (discussing the different bases for a State's exercise of extraterritorial jurisdiction).

assertions are normally resolved through the principles of comity.[140] As the U.S. Supreme Court recently described it, "[American] courts have long held that application of [American] antitrust laws to foreign anticompetitive conduct is nonetheless reasonable, and hence consistent with principles of prescriptive comity, insofar as they reflect a legislative effort to redress domestic antitrust injury that foreign anticompetitive conduct has caused."[141]

States have also established international agreements that have created methodologies for the exercise of jurisdiction over persons. These agreements include both multilateral agreements such as the European Cybercrime Convention[142] and bilateral agreements such as extradition treaties.[143] They provide a mechanism for sovereign States to assert rights over individuals in situations of conflicting claims.[144]

2. Obligations

The ability to exercise rights of legal persons also brings obligations to do so. Recall the maxim that States must prevent their territory from knowingly being used to harm the territory of another. That harm is almost always generated by some actor, taking some action. If States have the obligation to prevent known trans-boundary harm, they have to accept the corresponding obligation to exercise control and authority over those within their power who are causing that trans-boundary harm. This obligation applies to both State and non-State actors.

The ICJ provided insight into the application of this obligation to non-State actors in *Armed Activities on the Territory of the Congo*.[145] The Court was unwilling to assign responsibility to Zaire for not preventing the activities of certain armed groups because the government was not capable of doing so.[146] However, the clear implication of the Court's decision is that if the government had been capable, it would have had the obligation to do so.

---

140. Robert C. Reuland, Hartford Fire Insurance Co., *Comity and the Extraterritorial Reach of United States Antitrust Laws*, 29 TEX. INT'L L.J. 159, 161 (1994) ("In adopting a position that comity considerations may be relevant only in the case of a 'true conflict,' the Supreme Court effectively closes the door to the consideration of comity issues under any circumstances short of an actual conflict between U.S. and foreign law.").

141. F. Hoffmann-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 165 (2004) (emphasis omitted).

142. Convention on Cybercrime, *supra* note 92.

143. *E.g.*, Extradition Treaty between the United States of America and the United Kingdom of Great Britain and Northern Ireland, U.S.-U.K., Mar. 31, 2003, T.I.A.S. No. 07-426.

144. *See, e.g.*, Cohan, *supra* note 41, at 939–40 ("Membership in the United Nations and in other international organizations means that the participating state accepts the right of its fellow members to intervene in its domestic affairs if it has failed in its most fundamental obligations to protect its own citizens . . . ." (internal quotation marks omitted)); Worth, *supra* note 48, at 256 ("Article 12(2)(b) [of the Rome Statute] states that the Court will have personal (*ratione personae*) jurisdiction over the citizens of states that have become party to the [International Criminal Court].").

145. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, paras. 299–301 (Dec. 19).

146. *Id.*

C. *Application to Cyberspace*

One of the potential difficulties with applying sovereignty to cyberspace is the claim that cyberspace is a virtual world and does not lie within any national sovereignty.[147] In other words, skeptics claim that the activities that take place in cyberspace do not always fall under a State's jurisdiction.[148] The next two Subparts will analyze these arguments with respect to territory and persons.

1. Territory

Some have likened cyberspace to the commons, such as the high seas, and proposed that a similar legal regime should apply.[149] The argument is that because cyberspace does not fall within any State's territory, it is not subject to any State's sovereignty.[150] The authors of the *Tallinn Manual* responded to this issue by arguing that "although no State may claim sovereignty over cyberspace *per se*, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure."[151]

Cyber infrastructure is composed of servers, computers, cable, and other physical components.[152] These components are not located in cyberspace, but on some State's territory. It seems clear that a State has jurisdiction and exercises sovereign authority over these components that are located within its territorial boundaries. A State also exercises jurisdiction over cyber infrastructure outside its geographic boundaries if it exercises exclusive control over that cyber infrastructure, such as with cyber infrastructure on a State warship on the high seas.[153] The scope of territorial sovereignty in cyberspace includes the cyber infrastructure "located on a State's land area, in its internal waters, territorial sea and, where applicable, archipelagic waters, and in national airspace" but does not extend to its exclusive economic zone or on the continental shelf where States only exercise "sovereign rights."[154]

The law is at least settled enough with respect to cyber activities that the authors of the *Tallinn Manual* listed as its first "black letter" rule, "A State may exercise control over cyber infrastructure and activities within its sovereign

147. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1371 (1996) ("The power to control activity in Cyberspace has only the most tenuous connections to physical location.").

148. *See, e.g., Id.* at 1372 (arguing that "efforts to control the flow of electronic information across physical borders . . . are likely to prove futile").

149. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 517 (2003) ("[W]ith the intangible property of cyberspace, we can throw out our normal assumptions about private ownership of the resources and recognize that a commons system might be the most efficient use of the resource.").

150. *See* Johnson & Post, *supra* note 147, at 1370 ("The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.").

151. TALLINN MANUAL r. 1 cmt. 1.

152. *Id.* gloss.

153. *Id.* r. 5.

154. von Heinegg, *supra* note 7, at 128 & n.17.

territory."[155] One of the *Tallinn* authors has also written that "State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction."[156] Nor does connecting that infrastructure to the World Wide Web connote some kind of waiver of sovereignty.[157] In fact, the practice of States is just the opposite—the practice of States has made it clear that they will continue to exercise territorial sovereignty over their cyber infrastructure.[158]

This authority comes with corresponding duties and obligations. One of the primary obligations is that a State has an obligation not to knowingly allow its cyber infrastructure within its territory or under its exclusive control to cause trans-boundary harm.[159] This obligation has been accepted to apply to radio telecommunications[160] and was recently recognized as a rule by the authors of the *Tallinn Manual*.[161]

This obligation has also been stated in multiple official State comments. For example, according to China, sovereign States "have the responsibilities and rights to take necessary management measures to keep their domestic cyberspace and related infrastructure free from threats, disturbance, attack and sabotage."[162] Similarly, India has stated,

> By creating a networked society and being a part of [a] global networked economy, it is necessary for nation states to realise that they not only have a requirement to protect their own ICT infrastructure but at the same time have a responsibility to ensure that their ICT is not abused, either covertly or overtly, by others to target or attack the ICT infrastructure of another nation state.[163]

Likewise, Russia has stated that "States and other subjects of international law should refrain of [sic] such actions against each other and should bear responsibility at international level for such actions in information space, carried out directly, under their jurisdiction or in the framework of international organizations of their membership."[164] Finally, the U.S. government's 2011 International Strategy for Cyberspace calls on States to "recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet."[165]

---

155. TALLINN MANUAL r. 1.

156. von Heinegg, *supra* note 7, at 126.

157. *Id.*

158. DEPARTMENT OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 89, at 1.

159. Schmitt, *The Law of Cyber Warfare*, *supra* note 12, at 276.

160. *Developments in the Field of Information and Telecommunications*, *supra* note 8, at 3.

161. TALLINN MANUAL.

162. Kanuck, *supra* note 9, at 1591 (internal quotation marks omitted).

163. *Id.*

164. *Id.* at 1591 n.88.

165. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 37, at 10.

These and similar statements, combined with limited State practice, have led many commentators[166] to argue,

> States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states of cyberattacks that originated from within their borders.[167]

The kinds of acts that equate to trans-boundary harm might include attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy.[168] At this point, it is still unclear under the law as to whether the mere transit of data through a particular nation's infrastructure rises to the level of a prohibited activity, even if the data eventually results in harm to another State.[169]

Note that the obligation only triggers if the State from whose territory the harm originates has knowledge of the harm.[170] When States have knowledge of the harmful acts, they have a duty to stop them.[171] Knowledge might be imputed to the State if State agents or organs, such as intelligence or law enforcement agencies, know of the harm emanating from the State's cyber infrastructure, even if those agents or organs choose to not inform other agencies in the government.[172]

There may also be times when neither a State nor its organs or agents have actual knowledge but should have had knowledge, given the circumstances. In the ICJ's *Corfu Channel* case, the court held Albania liable for harm to England, even though there was no direct evidence that Albania knew of the harm. In that case, the court concluded that given the circumstances, Albania must have known about the emplacement of the mines that caused the harm.[173] The "must have known" standard is higher than a "should have known" standard but demonstrates that proving actual knowledge is not required. As for States who "should have known," international law is still unclear as to the obligation of such a State.[174] However, von Heinegg is willing to allow a rebuttable presumption of actual or constructive knowledge if "a cyber attack has been launched from cyber infrastructure that is

166. *E.g.*, David E. Graham, *Cyber Threats and the Law of War*, 4 J. NAT'L SEC. L. & POL'Y 87, 93–94 (2010); Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 62–63 (2009).

167. Sklerov, *supra* note 166, at 62–63.

168. *See* OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 37, at 12–14 (recognizing that cyberspace activities can have effects beyond borders and detailing initiatives that will be undertaken to protect the United States against threats posed by cyber criminals or States and their proxies).

169. von Heinegg, *supra* note 7, at 137.

170. *Id.* at 136.

171. *Id.* at 135–36.

172. *Id.* at 136.

173. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 19–20 (Apr. 9).

174. *See* von Heinegg, *supra* note 7, at 151 (speculating hypothetically about whether constructive knowledge is sufficient to establish a violation).

under exclusive government control and that is used only for non-commercial government purposes."[175]

There is currently an ongoing discussion as to whether a State's responsibility to prevent knowing cyber harm creates a duty to monitor networks in order to "know" when cyber harms exist.[176] In other words, if such a responsibility exists, if State A knows that its infrastructure is being used to cause trans-boundary harm to State B, State A has an obligation to stop the harm.[177] In order to effectively comply with that obligation, there is an emerging norm that State A has an obligation to monitor its cyber infrastructure and take proactive measures to prevent harm from emanating from cyber infrastructure over which State A exercises sovereignty.[178] However, this emerging norm is still quite controversial, particularly when considered in light of potential human rights obligations that might be compromised in the process of monitoring.[179]

Until that norm becomes generally accepted, target States will have to find ways to determine the level of knowledge of States from whose territory harmful cyber effects originate before allocating responsibility. In the current view of the United States,

> [Department of Defense (DoD)] adheres to well-established processes for determining whether a third country is aware of malicious cyber activity originating from within its borders. In doing so, DoD works closely with its interagency and international partners to determine: [(1)] The nature of the malicious cyber activity; [(2)] The role, if any, of the third country; [(3)] The ability and willingness of the third country to respond effectively to the malicious cyber activity; and [(4)] The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.[180]

In addition to the obligation to prevent trans-boundary harm, a State has an obligation to cooperate with the victim State in the event of adverse or unlawful cyber effects from cyber infrastructure located in its territory or under its exclusive governmental control when it may affect international peace and security.[181] A

---

175. *Id.* at 137. Note that von Heinegg clearly states that the presumption does not allow for attribution. *Id.*

176. *See generally* Jensen, *State Obligations*, *supra* note 127.

177. *See id.* at 13 (stating that in order to comply with the duty to control their cyber infrastructures, States have an emerging duty to monitor cyber activities within their territories in order to prevent or stop activities that are adversely or unlawfully affecting other States).

178. *Id.*

179. *Cf.* EKATERINA A. DROZDOVA, CIVIL LIBERTIES AND SECURITY IN CYBERSPACE 13 (2000), *available at* http://fsi.stanford.edu/sites/default/files/drozdova.pdf ("While a system for advanced monitoring, searching, tracking, and analyzing of communications may be very helpful against cyber crime and terrorism, it would also provide participating governments, especially authoritarian governments or agencies with little accountability, tools to violate civil liberties domestically and abroad.").

180. DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 8.

181. In addition to those circumstances mentioned above where the maintenance of international

State may also have a treaty obligation to establish criminal information sharing and criminal processing arrangements as a matter of domestic law.[182]

This obligation to cooperate is based on the U.N. Charter[183] and ICJ opinions,[184] and is also confirmed in the U.N. General Assembly's Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations.[185] The obligation to cooperate with respect to cyber incidents is also enshrined in the European Convention on Cybercrime, which has forty-two States parties and an additional eleven signatory States.[186]

This norm of cooperation only requires States to cooperate when the adverse or unlawful cyber incident originates from infrastructure within the territory or under its exclusive governmental control or when the unlawful cyber incident transits the cyber infrastructure in the State's territory or under its exclusive government control. Both conditions must be met for the duty to be applicable. No specific standard for the level of cooperation is clearly agreed upon, but the general consensus is that States must exercise good faith when fulfilling this duty.[187]

As an example, if a cyber incident originates in State A and threatens State B's critical infrastructure such that there is a threat to international peace and security, both State A and State B have a legal duty to cooperate to peacefully resolve that incident.

As with the obligation concerning trans-boundary harm, the obligation to cooperate also has a number of unresolved issues. Most relevant to this Article is the fact that historical State practice does not demonstrate that States accept the obligation to cooperate in any meaningful way.[188] Again, the 2007 situation between

---

peace and security is at risk, the duty to cooperate also applies to the solving of international problems of economic, social, cultural, or humanitarian character. U.N. Charter art. 1, para. 3. States also have a duty to cooperate in scientific investigation in Antarctica. The Antarctic Treaty, *supra* note 53, art. 2. The duty to cooperate also applies to the scientific investigation of outer space. Outer Space Treaty, *supra* note 55, art. 1. Finally, international cooperation applies to marine scientific research. U.N. Convention on the Law of the Sea, *supra* note 54, art. 143.

182. *See, e.g.*, Convention on Cybercrime, *supra* note 92, art. 26, para. 1 ("A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.").

183. U.N. Charter art. 1, paras. 1, 3; *Id.* art. 33, para. 1.

184. *See, e.g.*, Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, para. 102 (Apr. 20) (finding it vital for parties to comply with their procedural obligations under the 1975 Statute of the River Uruguay because cooperation is essential to the protection of the river).

185. G.A. Res. 2625 (XXV), *supra* note 80, at 123.

186. Article 23 requires that "[t]he Parties shall co-operate with each other" and provide mutual assistance, particularly with respect to investigations of cyber incidents. Convention on Cybercrime, *supra* note 92, art. 23.

187. *See* Kotzur, *supra* note 93, para. 16 ("One of the most basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith.").

188. *See* Schmitt, *The Law of Cyber Warfare*, *supra* note 12, at 273 ("A state's national interests undergird its consent or conduct .... States might seek, for example, to maximize power and influence at the expense of other states ....").

Estonia and Russia is instructive. Estonia found Russia's response to its queries and requests for assistance unhelpful and protective of Russian interests.[189]

2. Persons

The U.S. Department of Justice's recent indictment of five members of the Chinese Army for cyber hacking[190] represents a significant shift from the methodology States have traditionally used in dealing with State-sponsored cyber activities.[191] For the United States to move away from its normal diplomatic approach[192] and invoke domestic criminal law as a means of deterring State-sponsored cyber activities is a definite policy shift.[193] Certainly, it is improbable that the indictment will result in any convictions as China and the United States do not have an extradition treaty[194] and China has signaled no intention to honor such a request anyway. However, the idea that States will use domestic criminal law as a tool to deter other States who are engaged in harmful cyber activities is a potentially interesting development. The use of criminal law for non-State actors, on the other hand, is the norm, however ineffective.

It seems clear that in addition to State actors, "terrorist groups and even individuals, [sic] now have the capability to launch cyber-attacks, not only against military networks, but also against critical infrastructures that depend on computer

189. See Ruus, *supra* note 2 ("[T]he Estonian State Prosecutor made a formal investigative assistance request, which Moscow rejected, alleging that procedural problems prevented cooperation.").

190. Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html. China is, of course, not the only State conducting cyber activities. Recent media revelations concerning the United States' cyber activities have alleged widespread actions against both State and commercial entities. Simon Romero & Randal C. Archibold, *Brazil Angered Over Report N.S.A. Spied on President*, N.Y. TIMES, Sept. 2, 2013, http://www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html; David E. Sanger & Nicole Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*, N.Y. TIMES, Mar. 22, 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html; *Snowden NSA: Germany to Investigate Merkel "Phone Tap"*, BBC (June 4, 2014), http://www.bbc.com/news/world-europe-27695634; Jonathan Watts, *NSA Accused of Spying on Brazilian Oil Company Petrobras*, GUARDIAN, Sept. 9, 2013, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

191. *See* Schmidt & Sanger, *supra* note 190 ("[President Obama and Defense Secretary Chuck Hagel] have attempted to engage the Chinese in a dialogue over norms for operating in cyberspace, a careful diplomatic dance that has gone on for several years. But Monday's action by the Justice Department marked an attempt to publically shame the Liberation Army . . . .").

192. *See* Ellen Nakashima, *U.S. Publicly Calls on China to Stop Commercial Cyber-Espionage, Theft of Trade Secrets*, WASH. POST, Mar. 11, 2013, http://www.washingtonpost.com/world/national-security/us-publicly-calls-on-china-to-stop-commercial-cyber-espionage-theft-of-trade-secrets/2013/03/11/28b21d12-8a82-11e2-a051-6810d606108d_story.html (discussing the United States' diplomatic efforts to hold China accountable for cyber-espionage).

193. *See* Schmidt & Sanger, *supra* note 190 (describing how the Justice Department indicted five members of the Chinese People's Liberation Army and illustrating how this represents a U.S. policy shift on dealing with Chinese cyber activities).

194. Dominic Rushe, *Chinese Hackers Break into US Federal Government Employee Database*, GUARDIAN, July 10, 2014, http://www.theguardian.com/world/2014/jul/10/china-hackers-us-government-employee-database.

networks."[195] And the results of such actions can be catastrophic. "[M]alicious actors, state and non-state, have the ability to compromise and control millions of computers that belong to governments, private enterprises and ordinary citizens."[196] The threat is such that

> [t]he President's May 2011 International Strategy for Cyberspace states that the United States will, along with other nations, encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend these national security and vital national assets as necessary and appropriate.[197]

The fact that cyber operations may be initiated by a vast array of persons implicates the States from which those persons take those actions. Every time there is a victim-State, there is a State from which the action was initiated and often a State or States through which the activity passed. In each case, those States have not only the right to control their citizens and others who might be involved, but also the obligation to do so.[198] When persons take actions from within a State that harm another State, the State from which the harm originated has an obligation to try to stop those actions, once the State has knowledge.[199] If a State is monitoring its networks and knows in advance, it can act preemptively to stop that activity before it emanates from within its sovereign territory. Additionally, as stated above with respect to controlling actions, a State can take proactive measures to discourage non-State actors by "passing stringent criminal laws, conducting vigorous investigations, prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-States of cyberattacks that originated from within their borders."[200]

D. The Way Ahead

Applying a State's sovereign rights and obligations to persons with respect to cyber activities emphasizes the key role States must play in the way ahead for cyberspace. As the community of States moves forward, States will have to determine how the exercise of those sovereign rights and obligations can best be managed to accomplish each State's purposes.

For example, there are a number of issues revolving around the obligation to prevent trans-boundary harm. One of these issues stems from the fact that international law allows for some *de minimis* imposition on the rights of other States.[201] It is unclear generally what the limit of acceptable *de minimis* harm is, but

---

195. Liaropoulos, *supra* note 9, at 136 (citation omitted).

196. *Id.* at 137.

197. DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 2.

198. Jensen, *Sovereignty and Neutrality*, *supra* note 9, at 826–27.

199. *Id.*

200. Sklerov, *supra* note 166, at 62.

201. *See* Jutta Brunnée, *Sic utere tuo ut alienum non laedas*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 7 (2010) ("[T]he mere causation of transboundary harm does not transgress the *sic utere tuo* maxim.").

this is particularly unclear in cyberspace, where it is accepted that most cyber activities will not rise to the level of a use of force.[202] As time progresses, State practice will indicate what the acceptable amount of *de minimis* harm is and where that line is generally crossed. Currently, that line is quite high because States are unwilling to respond in forceful ways to cyber activities.[203] The shift in U.S. policy to apply domestic criminal remedies reflects that at least some States are not comfortable with the current paradigm. States' willingness to accept State-sponsored cyber activities, even those that are far below the use of force, seems to be waning. The future will undoubtedly bring more proactive measures to deter States from conducting cyber activities and reduce the acceptable level of *de minimis* cyber harm.

Another current issue that will likely come to the fore in the near future concerns the knowledge requirement for the trans-boundary harm obligation. While the law is clear that some form of knowledge, whether actual or constructive, is required for responsibility, the law is unclear as to the responsibility of a State that chooses not to invest in cyber capabilities on purpose, in an effort to remain blind to its obligations.[204] This issue of the level of knowledge, and responsibility to seek knowledge, will need to be resolved by State practice over time. As the duty to monitor and prevent continues to emerge, States will have to accept greater responsibility under a constructive knowledge standard and a State's ability to practice willful blindness will disappear. The pressures of the increasing availability of technology and the rising awareness of cyber activities will aid in this movement.

Finally, though there is a clearly recognized rule of international law on the acceptance of responsibility for trans-boundary harm, State practice in the cyber area has been inconsistent at best, and directly non-compliant in many cases.[205] Particularly in the area of cyber operations that are generated from within a State's borders, there is a mixed history on responsible States' willingness to accept responsibility.[206] Though this trend could actually go either way, it seems likely that the harms that are possible through cyber activities will eventually outweigh the benefits that States accrue by having freedom of action. Thus, particularly in light of the fact that non-State actors and even lone individuals can harness State-level violence through the use of cyber tools, States will soon find it in their best interest

---

202. *See* TALLINN MANUAL r. 11 (defining the term "use of force" in the cyber context as an operation the scale and effects of which are comparable to non-cyber operations that would qualify as a use of force).

203. *But see* DEPARTMENT OF DEFENSE, CYBERSPACE POLICY REPORT, *supra* note 105, at 4 ("Finally, the President reserves the right to respond using all necessary means to defend our Nation, our Allies, our partners, and our interests from hostile acts in cyberspace. Hostile acts may include significant cyber attacks directed against the U.S. economy, government or military. As directed by the President, response options may include using cyber and/or kinetic capabilities provided by [the Department of Defense].").

204. TALLINN MANUAL r. 93.

205. *See, e.g.*, discussion *supra* Part II.C.1 on Russia's unwillingness to assist Estonia after the 2007 cyber attacks.

206. *See, e.g.*, Sklerov, *supra* note 166, at 10 ("As may be expected, China and Russia reject these accusations.").

to regulate themselves in order to protect themselves not only from other States, but from non-State actors as well.

CONCLUSION

An analysis of the international doctrine of State sovereignty demonstrates that many of those norms are directly applicable to cyber operations and can easily be applied with respect to States. In fact, the recently published *Tallinn Manual* concludes that principles of sovereignty can be applied and does so apply them.[207]

However, there are still areas where State practice has presented difficulties, such as the area of accepting responsibility for trans-boundary harm, the emerging principles of a duty to monitor and prevent, and the duty to apply due regard to a State's cyber activities.

It seems clear, though, that the future will provide greater clarity as incidents of state cyber activities become more widespread and the information more available to the public. At that point, the way ahead is likely to demonstrate that the doctrine of sovereignty continues to apply to cyber operations.

207. TALLINN MANUAL R. 1.