Volume 10 | Issue 1 Article 5

1-29-2020

An Extraterritorial Human Right to Cybersecurity

Ido Kilovaty
University of Tulsa College of Law

An Extraterritorial Human Right to Cybersecurity

Cover Page Footnote

Frederic Dorwart and Zedalis Family Fund Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School.

The author wishes to thank Jeff Kosseff for his valuable feedback on this piece.

AN EXTRATERRITORIAL HUMAN RIGHT TO CYBERSECURITY

IDO KILOVATY*

INTRODUCTION

The private and public sectors have been experiencing devastating cybersecurity incidents for at least two decades now.[1] Sony,[2] Yahoo!,[3] Equifax,[4]

---

* Frederic Dorwart and Zedalis Family Fund Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. The author wishes to thank Jeff Kosseff for his valuable feedback on this piece.

[1] *See, e.g.,* Taylor Armerding*, The 18 Biggest Data Breaches of the 21st Century,* CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html/.

[2] Andrea Peterson, *The Sony Pictures Hack, Explained,* WASH. POST (Dec. 18, 2014) https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/, ("Hackers broke into the computer systems of Sony Pictures entertainment in October. The attackers stole huge swaths of confidential documents from the Hollywood studio and posted them online in the following weeks . . . . Multiple reports suggest U.S. government officials believe the attack is tied to the North Korean government, who expressed outrage over the Sony-backed film 'The Interview,' an action-comedy centered on an assassination plot against North Korean leader Kim Jong Un.").

[3] Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack,* N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html, ("Digital thieves made off with names, birth dates, phone numbers and passwords of users that were encrypted with security that was easy to crack . . . investigators believe the attackers behind the 2013 breach were Russian and possibly linked to the Russian government.").

[4] Kate Fazzini, *The Great Equifax Mystery: 17 Months Later, the Stolen Data Has Never Been Found, and Experts Are Starting to Suspect a Spy Scheme,* CNBC (Feb. 13, 2019), https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html, ("In a brazen cyberattack, somebody had stolen sensitive personal information from more than 140 million people, nearly half the population of the U.S. . . . Most experts familiar with the case now believe that the thieves were working for a foreign government and are using the information not for financial gain, but to try to identify and recruit spies.").

the Democratic National Committee (DNC),[5] Office of Personnel Management,[6] and many others represent the share of intrusion victims originating from abroad. Sony, for example, became the target of a data breach that allegedly originated in North Korea, protesting the release of *The Interview*—a comedy movie depicting the assassination of Kim Jong-un.[7] Similarly, the DNC experienced a cybersecurity incident when Russian hackers, affiliated with the Kremlin, gained unauthorized access to controversial e-mails that led to political turmoil in the U.S., allegedly swaying the public opinion and affecting the outcome of the 2016 presidential election.[8]

Given the international nature of most of these incidents—originating from abroad and allegedly orchestrated by a state actor—recourse to international law ought to be intuitive.[9] After all, international law is the body of law regulating and shaping acceptable behavior among nations.

However, as this Article will demonstrate, general international law suffers from a few fatal flaws that make it a less-than-perfect candidate to stymie the consequences of offensive cyberspace behavior, particularly as it victimizes private sector entities and individuals.[10]

While international law is seemingly ineffective in deterring or regulating transnational offensive cyberspace behavior, this Article will propose an alternative that is centered around protecting the individual from foreign cyberattacks through the application of international human rights law across borders, as well as its development to meet today's global cybersecurity threats.[11] Thus far, the majority of scholarship on transnational cyber operations has focused on the victim state's rights, such as sovereignty and territorial inviolability to delegitimize these operations.[12] Yet, debates on the precise

---

[5] Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed its Emails to Wikileaks,* WASH. POST (July 13, 2018), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

[6] Devlin Barrett, *Chinese National Arrested for Allegedly Using Malware Linked To OPM Hack*, WASH. POST (Aug. 24, 2017), https://www.washingtonpost.com/world/national-security/chinese-national-arrested-for-using-malware-linked-to-opm-hack/2017/08/24/746cbdc2-8931-11e7-a50f-e0d4e6ec070a_story.html. ("Court papers filed against Yu Pingan do not mention the OPM, but they do suggest a connection between the two. The OPM hack is considered one of the worst-ever computer breaches of U.S. government computer systems because the hackers were able to access a huge volume of information from security clearance forms filed by federal workers and contractors.").

[7] Peterson, *supra* note 2.

[8] SPECIAL COUNSEL ROBERT S. MUELLER, III, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 1 (Mar. 2019), ("The Russian government interfered in the 2016 presidential election in a sweeping and systematic fashion. Evidence of Russian government operations began to surface in mid-2016. In June, the Democratic National Committee and its cyber response team publicly announced that Russian hackers had compromised its computer network. Releases of hacked materials—hacks that public reporting soon attributed to the Russian government—began that same month.").

[9] *See generally* Mary Ellen O'Connell, *Cyber Mania,* CYBER SECURITY AND INTERNATIONAL LAW: MEETING SUMMARY (CHATHAM HOUSE, MAY 29, 2012).

[10] *See* Michael Schmitt, *Grey Zones in International Law of Cyberspace,* 42 YALE J. INT'L L. ONLINE 1 (2017) (highlighting the gaps and loopholes in international law as applied to cyberspace).

[11] *See generally* Oona Hathaway et al., *Human Rights Abroad: When Do Human Rights Treaty Obligations Apply Extraterritorially?*, 43 ARIZ. ST. L. J. 389 (2011).

[12] *See e.g.*, Edwin Djabatey, *U.S. Offensive Cyber Operations Against Economic Cyber Intrusions: An International Law Analysis: Part II*, JUST SECURITY (July 16, 2019) (arguing that some U.S. offensive cyber operations against economic cyber intrusions could violate the principle of sovereignty).

contours of sovereignty, its commonly understood high threshold, reliance on state's rights (as opposed to rights of individuals), and the lack of concepts that fit squarely with the realities of cyberspace, make it an ineffective tool to address the victimization of private entities.

By focusing on individual, non-state victims, international human rights law is able to constrain offensive state behavior in cyberspace that interferes with the rights afforded to these victims—whether the right to privacy, self-determination, due process, or freedom of expression or opinion. However, it is the view of this Article that further development of international human rights law is required, particularly in the form of a new human right to cybersecurity. To be clear, whenever international law is mentioned in this Article, it is meant to the exclusion of international human rights law. While international law contains a broad variety of discrete bodies of law, international human rights law differs in significant ways from general international law, as will be further explored in this Article.

By proposing an extraterritorial application of international human rights law as a solution, this Article is also mindful of the challenges that such a proposition entails. For example, while international human rights law is an established body of law that enjoys near-universal acceptance, states operating in cyberspace rarely acknowledge the legal and ethical constraints that shape their activities in that domain.[13] Though, even if some states decide to acknowledge and accept the authority of international human rights law in cyberspace, a more significant conundrum that remains is whether such states are under obligation to respect the human rights of foreign individuals located abroad. Thus, this inquiry is far from hypothetical, as the mere extraterritoriality of human rights obligations may affect how states use offensive cyber operations across borders.

Assuming the international community accepts the extraterritorial application of international human rights law, this may still be insufficient in the context of cybersecurity. Once extraterritoriality is an established fact, the content of the human rights themselves may become ambiguous. Surely, privacy, freedom of expression and opinion, self-determination, and due process are all valuable rights. But what about the right to access the internet itself, or the right to cybersecurity (i.e., the protection afforded to individuals against cyberattacks in general)? As this Article will demonstrate, cybersecurity concerns may not be entirely alleviated by the existing human rights.

This Article will explore the gaps and ambiguities of international law in protecting non-state victims, the extraterritoriality of human rights as a solution, and the difficult challenges that would nonetheless persist. The Article is structured as follows. In Part I, this Article will look at international law in

---

[13] *See* Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice,* 112 AM. J. INT'L L. 583, 648 (2018) (arguing that states engaged in offensive cyberspace operations often "develop a policy of optionality toward the application of international law . . . a deliberate strategy of treating the applicable international law framework as optional, in the sense that states may choose whether or not to invoke the legal discourse of international rights and obligations in their mutual interactions in cyberspace"). Compare these with nations who have acknowledged the applicability of international law to cyberspace (France, Australia, Estonia, United Kingdom, Netherlands). *See* Michael Schmitt, *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis,* JUST SECURITY (Oct. 14, 2019).

general, demonstrating that its basic tenets and assumptions make it dysfunctional in the global cybersecurity context. In Part II, this Article will propose an extraterritorial application of international human rights law as a potential solution to the inadequacy of international law. In Part III, this Article will assess the primary challenges arising from the application of international human rights law across borders. Primarily, these challenges surround territoriality, the content of existing human rights, and the need for a human right to cybersecurity. This Article will propose ways to overcome these challenges. Part IV will conclude.

I. INTERNATIONAL LAW AND TRANSNATIONAL CYBERSECURITY INCIDENTS

As cybersecurity becomes a national security concern,[14] the resort to international law appears intuitive. After all, international law does safeguard certain national security interests that states have. The principles of sovereignty,[15] non-intervention,[16] and the prohibition on the threat or use of force[17] are only a few examples where international law accounts for national security. However, when transposed into cyberspace, these principles and prohibitions do not fit quite as well. What does *sovereignty* mean in a domain that lacks territory? Is election interference through cyberspace a violation of the principle of *non-intervention*? At what point does a data breach constitute a *use of force*? These are some of the most perplexing questions in the context of cybersecurity as national security.

A. *WHAT IS SOVEREIGNTY ANYWAY?*

While many would claim that sovereignty is a cornerstone principle of international law, the precise contours of such principle are highly contested and misunderstood.[18] The UN Charter for example, provides that "[t]he Organization [UN] is based on the principle of the sovereign equality of all its Members."[19]

---

[14] *See e.g.*, THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 11 (2018) ("Computer hacking conducted by transnational criminal groups poses a significant threat to our national security."); Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace*, 8 J. NAT'L SECURITY L. & POL'Y 503, 518 (2016) (quoting the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: "the Internet [may] be abused to interfere with the rights of others, national security, or public order").

[15] *See e.g.*, U.N. Charter art. 2(1) ("The Organization is based on the principle of the sovereign equality of all its Members."); Samantha Besson, *Sovereignty*, OXFORD PUB. INT'L L. ¶ 56 (last updated Apr. 2011) ("In international law, internal sovereignty is used to mean the supreme authority within a territory or the ultimate power within that territory.").

[16] *See e.g.*, U.N. Charter art. 2(7) ("Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state . . . .").

[17] *See* U.N. Charter art. 2(4) ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

[18] *See* Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1579 (2017) ("Sovereignty is a funny thing. It is allegedly the foundation of the Westphalian order, but its exact contours are frustratingly indeterminate.").

[19] U.N. Charter art. 2(1).

Another widely accepted understanding of sovereignty was articulated by the *Island of Palmas* arbitral award in 1928,[20] where the panel observed that sovereignty "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."[21]

While sovereignty is based largely on territorial notions, it is not out of the question that it applies equally to cyberspace. The *Tallinn Manual 2.0,* a work of a group of experts at the NATO Cooperative Cyber Defence Centre of Excellence translating existing international law to cyberspace, proclaimed that "*[t]he principle of State sovereignty applies in cyberspace*"[22] and that states "*must not conduct cyber operations that violate the sovereignty of another State.*"[23]

However, the application of sovereignty to cyberspace does not necessarily lead to any more clarity on the relationship between sovereignty and cybersecurity. For example, can sovereignty be violated if the target of a cybersecurity incident is not a state actor, but a private entity? What kinds of incidents and effects violate sovereignty? Can non-state actors directly violate sovereignty through cyberspace? This lack of clarity may inadvertently lead to an over-expansive view of what sovereignty means in cyberspace. Some argue that "*any* action occurring within the territory of another State without that State's permission"[24] would violate the "sovereign inviolability" of that state. This view would lead to the conclusion that any cybersecurity incident across borders is suspect of violating international law. In response, victim states could potentially overuse countermeasures to deter such attacks,[25] and increase the risk of escalation as a result.

At the other end of the spectrum are those who claim that sovereignty is a primary rule of international law, meaning that it is effectuated and enforced through secondary rules that are afforded greater granularity.[26] According to that view, sovereignty cannot be seen as a principle that can be violated directly, but rather as an idea that international law protects through specific norms, principles, and institutions. For example, the principle of non-intervention is often seen as the secondary rule through which sovereignty is enforced.

---

[20] Island of Palmas Case (Netherlands, U.S.) 2 R.I.A.A. 829 (Perm. Ct. Arb. 1928).

[21] *Id*. at 838.

[22] THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 11 (Michael Schmitt ed.) ("Rule 1") [hereinafter TALLINN MANUAL] (emphasis added).

[23] *Id.* at 17 ("Rule 4") (emphasis added).

[24] *See* Robert Taylor, *Cyber, Sovereignty, and North Korea – And the Risk of Inaction,* JUST SECURITY (Oct. 31, 2017), https://www.justsecurity.org/46531/cyber-sovereignty-north-korea-risk-inaction/.

[25] Michael Schmitt, *In Defense of Sovereignty in Cyberspace*, JUST SECURITY (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/ ("Countermeasures are proportionate actions by the 'injured' state that would be unlawful but for the fact that they are designed to put an end to the 'responsible' state's unlawful conduct, in this case a sovereignty violation.").

[26] Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639, 1650 (2017) ("The question at hand is whether the principle of sovereignty operates as a primary rule of customary international law, imposing an obligation on States to respect the inviolability of other States' territories.").

B. *THE PRINCIPLE OF NON-INTERVENTION*

International law prohibits external intervention in the domestic and foreign affairs of another state. While the history of international affairs regarded intervention as a legitimate tool of influence, international law has gradually come to delegitimize its use. In the *Corfu Channel* case, the International Court of Justice (ICJ) explained that "the alleged right of intervention as the manifestation of a policy of force, such as has, in the past, given rise to the most serious abuses and as such cannot, whatever be the present defects in international organization, find a place in international law."[27] Therefore, the principle of non-intervention "forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States."[28] Non-intervention is a fundamental principle of international law—"part and parcel of customary international law"—and can be found throughout different instruments of international law, with slight variations.[29]

But what does non-intervention mean in the context of global cybersecurity and increasing numbers of state-sponsored cyberattacks? The answer is not straightforward. Non-intervention, like many other principles of customary international law, suffers from an absence of authoritative and comprehensive doctrine, making it immensely difficult to apply to transnational cyber operations.[30] At the heart of the principle is the prerequisite that interference be "coercive." Intervention, the International Court of Justice explains, is "wrongful when it uses methods of coercion."[31] While the Court did not expand on the notion of coercion, it was understood that intervention is wrongful under international law when it is "forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."[32]

The contours of non-intervention raise some serious limitations on its applicability to transnational cyber operations. For example, considering the reciprocal security vulnerability concept, what if the target of an incident is a prominent private entity, resulting in a national security crisis? The principle may not apply since no state was deprived of its prerogative in making decisions on domestic or foreign affairs.

To the degree that a state-sponsored cybersecurity incident results in serious kinetic effects (deaths, injuries, or damage to physical property) it could be considered to be in violation of Article 2(4) of the UN Charter, prohibiting the

---

[27] Corfu Channel (U.K. v. Alb.), Judgement, 1949 I.C.J. Rep. 4, ¶ 35 (Apr. 9).

[28] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgement, 1986 I.C.J. Rep. 14, ¶ 205 (June 27) [hereinafter *Nicaragua*].

[29] *Id.* at ¶ 202; *See* Philip Kunig, *Intervention, Prohibition of*, OXFORD PUB. INT'L L. ¶ 7 (last updated Apr. 2008), http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434.

[30] *See e.g.*, Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L SECURITY J. 146 (2018) ("Generally, the norm of non-intervention would protect the victim state from physical intrusions by another state seeking private information." Conversely, some transnational cyberspace operations "deeply challenge the traditional understanding of what constitutes wrongful 'intervention.'").

[31] *Nicaragua*, *supra* note 28.

[32] 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 432 (Robert Jennings & Arthur Watts eds., 2008).

use of force,[33] entitling the victim state to invoke the right to self-defense if the use of force reaches the level of an *armed attack.*[34] However, since the vast majority of cybersecurity incidents are non-coercive and non-kinetic, as their purpose is primarily to access private or secret data, the principle of non-intervention and the prohibition on the use of force may not be relevant.[35] Arguably, non-intervention may still be relevant in cybersecurity should coercion be substituted by another standard.[36]

C. *RECIPROCAL SECURITY VULNERABILITY & OTHER SYSTEMATIC PROBLEMS*

Sovereignty, non-intervention, and the prohibition on the use of force may provide sufficient evidence of the inadequacy of international law in dealing with the reciprocal security vulnerability problem engulfing most state-sponsored cyber operations. However, the idea of "reciprocal security vulnerability" suggests that there may be some deeper problems with traditional international law and its ability to address transnational cybersecurity incidents.

Reciprocal security vulnerability, a problem in cybersecurity introduced by Andrea Matwyshyn, illustrates the vulnerability of both the private and public sectors to cyberattacks. Critical infrastructure systems "blend private and public-sector elements, simultaneously impacting both national security and consumer protection concerns,"[37] and therefore a clear distinction between the two sectors is impractical. This blurred line between private and public is not normally a concept that international law grapples with. For example, the attack on Sony targeted a private sector actor, however, the impacts on national security and foreign affairs were substantial.[38] The reasons why international law is not capable of responding to the reciprocal security vulnerability problem are rooted in its basic structure and defining characteristics, laid out below.

Perhaps the most plausible explanation of why reciprocal security vulnerability is not on international law's agenda is because international law is predominantly concerned with the rights of states, not the private sector. States are the objects and subjects of international law simultaneously.

---

[33] *See* U.N. Charter art. 2(4), ¶ 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

[34] *See Nicaragua*, *supra* note 28, at ¶191 (where the ICJ notes that an armed attack is "the most grave form of the use of force"); *See also* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.").

[35] *See* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 698, 705 (2014) ("Preoccupation with cyber armed attacks is counter-experiential. Few, if any, cyber operations have crossed the armed attack threshold," though there may be cyber operations that "violate the principle of non-intervention, and accordingly qualify as internationally wrongful acts.").

[36] *See generally* Ido Kilovaty, *The Elephant in The Room: Coercion*, 113 AM. J. INT'L L. UNBOUND 87 (2019).

[37] Andrea M. Matwyshyn, *Cyber!*, 2017 BYU L. REV. 1109, 1122 (2017).

[38] *See* Ellen Nakashima, *Why the Sony Hack Drew an Unprecedented U.S. Response Against North Korea*, WASH. POST (Jan. 15, 2015), https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html.

International law is largely a system of law that applies in the relationship between states. If state A breaches computer networks belonging to state B, then state A may be responsible for a violation of international law. However, as reciprocal security vulnerability illustrates, such isolated incidents are rare, and usually many more actors than the two immediate states are involved. For example, state A may attack state B's servers, but such an attack may also influence corporations using government databases, individuals whose private data got compromised, and civilians who may experience fear and anxiety because of a foreign cyberattack.

The concept of reciprocal security vulnerability brings these private entities and individuals into the equation, meaning that a body of law that isolates only two state actors from the rest is ignoring the bigger picture, in which non-state actors, typically individuals and private-sector entities, are the ones victimized by foreign state-sponsored cyberattacks. Therefore, to the extent that private sector entities or individuals are involved, international law is largely irrelevant. The exception to that is international human rights law, which obligates states to respect, protect, and ensure certain duties vis-à-vis individuals, which will be discussed further in Part II. International human rights law may prove effective in considering this bigger picture.

Second, international law currently does little to tell states how to promote their cybersecurity and privacy of their citizens. While international law protects the vital interests of states, such as sovereignty and territorial integrity, it does little to guide states in how private information ought to be protected, or what the state's role is in promoting the information security of its private sector and citizens. According to international law, the degree to which a state invests in its information security, or that of the private sector, is wholly under that state's discretion.

Third, many of international law's norms and principles assume territoriality. While information technology (IT) infrastructure is indeed located on physical territory, there are certain scenarios in which the reliance on territoriality may make international law irrelevant and ineffective. Consider cloud computing, where servers storing data may be located anywhere in the world. If state A uses cloud computing services to store certain data, and the servers are located abroad, the focus on territoriality would be beside the point.[39]

This scenario is far from hypothetical. The *United States v. Microsoft* (Microsoft-Ireland) case in the U.S. Supreme Court revolved around a Stored Communications Act warrant, requiring that Microsoft disclose data stored on a server in Ireland.[40] This has eventually led to Congress passing the Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[41] which purported to create a system by which U.S. law enforcement could access data stored abroad by

---

[39] Sharon Bradford Franklin, *The Microsoft-Ireland Case: A Supreme Court Preface to the Congressional Debate*, LAWFARE (Feb. 22, 2018), https://www.lawfareblog.com/microsoft-ireland-case-supreme-court-preface-congressional-debate ("In our interconnected world, the electronic data that we create may be stored far away from us, without regard for national boundaries. If our data become relevant to legitimate law enforcement investigations, the borderless nature of digital data can create obstacles for government investigators and the tech companies who receive government requests for their customers' electronic data.").

[40] *See* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (per curiam).

[41] CLOUD Act, S. 2383, H.R. 4943, 115th Cong. (2018).

electronic communication service and remote computing service providers.[42] The CLOUD Act has also authorized the U.S. government to enter into executive agreements between the U.S. government and "trusted foreign partners"[43] to allow these partners to access important digital evidence related to serious crime committed abroad. The Microsoft-Ireland case demonstrates that governments are themselves struggling in applying territorial mechanisms on issues that are extraterritorial by nature.

International human rights law can alleviate these three challenges. International human rights law protects primarily individuals, rather than states, it may offer guidance through more specific (though imperfect) obligations, and the rights can be applied personally rather than territorially, through a robust doctrine of extraterritoriality.

II. INTERNATIONAL HUMAN RIGHTS LAW AND TRANSBORDER CYBERATTACKS

Before World War II, international law had largely regulated interactions between states.[44] The aftermath of World War II was a pivotal moment for international law, when as many as sixteen multilateral human rights treaties were concluded, ensuring that states could no longer "act within their own borders with absolute impunity."[45] Therefore, whenever states engage in certain interactions with or affecting their own citizens,[46] they are likely to be bound by certain human rights obligations deriving from either treaties or customary international law. Indeed, most treaties contain provisions limiting their "geographical or jurisdictional reach,"[47] which could apply in certain extraterritorial scenarios.

Article 2(1) of the International Convention on Civil and Political Rights (ICCPR) reads: "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant."[48] While the plain meaning of "within its territory" and "subject to its jurisdiction" may appear conjunctive at first, the practice that had crystalized around this scope of application reflects a

---

[42] U.S. DEP'T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 16 (Apr. 2019).

[43] *Id.* at 2.

[44] Frans Viljoen, *International Human Rights Law: A Short History*, 46 UN CHRONICLE (Jan. 2009) ("For many centuries, there was no international human rights law regime in place. In fact, international law supported and colluded in many of the worst human rights atrocities.").

[45] Hathaway, *supra* note 11, at 389.

[46] *See* John Humphrey, *The International Law of Human Rights in the Middle Twentieth Century,* in THE PRESENT STATE OF INTERNATIONAL LAW AND OTHER ESSAYS WRITTEN IN HONOUR OF THE CENTENARY CELEBRATION OF THE INTERNATIONAL LAW ASSOCIATION (1973) ("Human rights were—and indeed still are—essentially a relationship between the State and individuals—usually its own citizens—residing in its territory . . . considered to fall within domestic jurisdiction and hence beyond the reach of international law, the norms of which governed the relations of States only.").

[47] Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE (Nov. 14, 2013), https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy.

[48] International Covenant on Civil and Political Rights art. 2(1), *opened for signature* Dec. 19, 1996, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976).

disjunctive approach.[49] Therefore, the obligations enumerated in the ICCPR refer to individuals either within a territory of a state party or subject to its jurisdiction.

This disjunctive interpretation allows for some form of extraterritoriality in very limited circumstances.[50] For example, the Human Rights Committee (HRC), in a comment reflective of customary international law, stated that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[51] This standard has been guiding certain international institutions over the years, and was later applied in a Human Rights Council resolution on remote drone strikes.[52] No longer could counter terrorism measures be unconstrained by any law, and states engaged in these operations have become bound by "international law, including the Charter of the United Nations, international human rights law and international humanitarian law."[53]

Adopting the HRC extraterritoriality standard of "within the power of effective control," the *Tallinn Manual* clarifies that certain human rights apply "beyond a State's territory" in cases where that state "exercises 'power and effective control.'"[54] According to the *Tallinn Manual*, this control may be "over territory (spatial model) or over individuals (personal model)."[55] This approach, when applied to cyberspace, ignores a different kind of power that states may exert over individuals online. Indeed, the *Tallinn Manual* International Group of Experts have acknowledged this loophole in the law on extraterritoriality which disregards new forms of control online.[56] It notes that "the International Group of Experts could achieve no consensus as to whether State measures that do not involve an exercise of physical control may qualify as 'power or effective control.'"[57] Mainly, such lack of consensus has to do with the lack of state practice and *opinio juris* on the question, suggesting that there may be room for a legal evolution on the topic in the future.[58]

While this kind of extraterritoriality may seem desirable to keep state action abroad in check, this issue remains highly contested in the U.S., as American officials have historically rejected an extraterritorial application of human rights

---

[49] *See* Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace*, 8 J. NAT'L SEC. L. & POL'Y 503, 507 (2016) ("Increasingly, the terms 'within its territory and subject to its jurisdiction' are being interpreted in their disjunctive, rather than conjunctive sense, at least as concerns the State's negative obligation to refrain from violating rights. Thus, the State is bound by international human rights law in relation to individuals outside of its territory but otherwise under its jurisdiction.").

[50] *See* Deeks, *supra* note 47 at 1 ("Many other states, as well as the ICCPR treaty body, assert that the ICCPR applies either when a person is within the territory of a state party *or* is subject to a state's jurisdiction (as when a state detains a non-national abroad).").

[51] The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, Rep. of the Human Rights Comm. on its Eightieth Session, CCPR/C/21/Rev.1/Add. 13, at 4 (May 26, 2004).

[52] G.A. Res. 25/3, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development (Mar. 24, 2014).

[53] *Id.* at 1.

[54] TALLINN MANUAL, *supra* note 22, at 184.

[55] *Id.* (internal citations omitted).

[56] *Id.* at 185.

[57] *Id.*

[58] *Id.*

treaties.[59] In an infamous legal memo, then State Department Legal Adviser, Harold Koh, rejected the interpretation that the International Covenant on Civil and Political Rights imposes positive obligations extraterritorially.[60] According to Koh, protecting "persons under the primary jurisdiction of another sovereign otherwise could produce conflicting legal authorities," and therefore, the ICCPR ought to only impose extraterritorial obligations in "exceptional circumstances" where there is "effective control over a particular person or context without regard to territory."[61] In comparison, positive obligations (to ensure human rights) which require affirmatively protecting individuals, should only apply to individuals "both within the territory and subject to the jurisdiction" of the state involved.[62] While Koh's memo was ultimately not adopted by the administration, it did influence the official U.S. position on the matter.[63]

The contentions on extraterritoriality, while recent, predate the majority of cybersecurity incidents affecting national security. At present, state-sponsored cyberattacks may affect the rights of individuals without the attacking state exerting any effective control or jurisdiction over these individuals, simply because new technologies can seriously interfere with the enjoyment of rights. At its conception, international human rights law could not envision that states would become capable of interfering with and violating protected human rights enumerated in various treaties and customary international law. Therefore, the same international human rights law does not offer a robust understanding of extraterritoriality in light of transborder cybersecurity threats and power relations online. It may therefore be useful to conceptualize international human rights law as a regulating force for transborder cyberattacks.

A. *REGULATING ACROSS BORDERS*

International human rights law already protects individuals from their own government's overreach. Nationals of State A may already enjoy their rights vis-à-vis the government of State A. Examples relevant to cybersecurity are the

[59] *See* Charlie Savage, *U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad,* N.Y. TIMES (Mar. 6, 2014), https://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html?_r=0.

[60] U.S. DEP'T OF STATE, OFF. OF THE LEGAL ADVISER, MEMO. OPINION ON THE GEOGRAPHIC SCOPE OF THE INT'L COVENANT ON CIVIL AND POL. RTS. 55-56 (Oct. 19, 2010).

[61] *Id.*

[62] *Id.*

[63] Ohlin, *supra* note 18, at 1587.

rights to privacy,[64] freedom of expression,[65] freedom of opinion,[66] due process,[67] and self-determination.[68] State A could run afoul of its international obligations if it were to surveil its nationals, interfere with their freedom of expression, or violate their right to self-determination. While some derogations are permitted in "time[s] of public emergency which threatens the life of the nation"[69] the general expectation is that state parties comply with their treaty obligations most of the time.

Furthermore, even if a robust extraterritoriality model for cyberspace and other new technologies is widely adopted, this would not necessarily expose states to automatic liability for alleged human rights violations abroad. Human rights, like any other duties and rights, are not absolute. Extraterritoriality will simply mean that states will be required to offer substantial justification for their actions within the accepted exceptions contained in human rights treaties, which involve questions such as "is the interference prescribed by law; does it serve a legitimate aim; is it proportionate to that aim."[70]

---

[64] *See* Ryan Goodman, *The Koh Memo's Impact on the Current US Position (A Reply, in Part, to Ben Wittes)*, JUST SECURITY (Mar. 11, 2014), https://www.justsecurity.org/8124/koh-memos-impact-current-position-a-reply-part-ben-wittes/ ("Agree with the Koh Memorandum or not, it appears to have already altered the position that the United States has taken toward its reporting obligations under the International Covenant on Civil and Political Rights (ICCPR). Indeed, if you are a reader who flatly opposes the Memo's legal conclusions that the ICCPR imposes extraterritorial obligations, you would not be well-advised by anyone who tells you that the Memo has been "ignored" or doesn't actually "represent the considered view of the Legal Adviser's office.").

[65] *See* G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 19); (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 19(2), Dec. 19, 1996, T.S. No. 14668 (adopted by the General Assembly of the United Nations); European Convention on Human Rights art. 10(1), June 1, 2010, 14 C.E.T.S. 194; American Convention on Human Rights art. 13(1), Inter-Am. Comm'n H.R., Report (2011). *See also* TALLINN MANUAL, *supra* note 22, at 182 ("At the time international human rights law norms emerged it was recognised, for example, that the right to freedom of expression (Rule 35) extended to 'any' media, a reference that accommodates technological advancements, such as the emergence of cyber-enabled expression.").

[66] G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 19 (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 19(1), Dec. 19, 1996, T.S. No. 14668 (adopted by the General Assembly of the United Nations); Association of Southeast Asian Nations Human Rights Declaration art. 22 (Nov. 19, 2012).

[67] G.A. Res. 217 (III) A, Universal Declaration of Human Rights arts. 9–11 (Dec. 10, 1948); G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights arts. 9–11, 14–15 (Mar. 23, 1976).

[68] G.A. Res. 2200 (XXI) A, International Covenant on Economic, Social and Cultural Rights art. 1(2) (Jan. 3, 1976) ("All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development.").

[69] G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights art. 4(1) (Mar. 23, 1976) (alteration in the original).

[70] Marko Milanovic, *Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?*, EJIL: TALK! (Nov. 28, 2013), http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial-interferences-with-privacy/; *See also* Rona & Aarons, *supra* note 14, at 524–5 ("Any restriction on human rights in cyberspace must be 'provided' or 'prescribed by law' which meets 'certain minimum qualitative requirements of clarity, accessibility, and predictability.' No interference can take place except in cases envisaged by the law and relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. Limitations or restrictions on human rights may only be lawful if they serve a legitimate purpose, which includes protection of the rights or reputations of others; national security, public order, public health or morals. Where restrictions are justified, any interference must be limited to what is necessary and proportionate to achieve a legitimate aim or objective. Restrictions must be applied narrowly to avoid a legitimate objective being used as a pretext for an illegitimate restriction on human rights.") (internal citations omitted).

The concept of states owing certain duties toward their own nationals is straightforward. But extraterritoriality is taking these duties a step further – what if State A decides to interfere through cyberspace with the right to privacy belonging to nationals of State B located in the territory of State B?[71] Under that scenario, international law will have little to say as State B itself is not a target of the attack and international law offers no guidance on how the nationals of State B ought to be protected. Moreover, whatever international law offers may be contentious when applied to a situation where the attack targets a cloud server located in State C. The complexity of facts and contexts surrounding transborder cyber operations may actually lead to too many legal questions that are not necessarily easily resolved.[72] Moreover, new technologies create a disconnect between the geographical location of interference and the geographical location of the individual whose rights may have been violated.[73]

Surely, states can enter bilateral or multilateral agreements on the rules of conduct and sanctions for engaging in harmful cyber operations, whether in the form of a binding treaty or an informal agreement.[74] Such treaties may be desirable insofar as they protect the interests of individuals. But in the absence of such treaties, and considering the informality and incompleteness of existing agreements,[75] international human rights law may offer a baseline of what boundaries exist in the conduct of transnational cyber operations.

While the role of international human rights law in protecting humans cannot be overstated, the same body of law may also protect other private sector actors, such as corporations and organizations. Indirectly, international human rights law may protect these private sector entities by framing the violation as implicating the human rights of individuals affiliated with the targeted entity or

---

[71] *See* Ohlin, *supra* note 18, at 1586 (A good example of this is Russia attacking the DNC, exfiltrating e-mails belonging to DNC officials. Under the narrow territoriality interpretation, Russia would owe no obligation to respect and ensure the human rights to privacy of U.S. citizens. However, extraterritoriality may require that states abide by their obligation to respect and ensure the right to privacy of foreigners, under certain circumstances.).

[72] TALLINN MANUAL, *supra* note 22 at 593 ("The involvement of multiple states, including a number of states from whose territory the operation might have originated, the routing states, and several victim states raises difficult questions of allocating state responsibility, addressing conflict of laws (relating to criminal and civil liability), and applying the laws governing the use of force (e.g., whether one should evaluate cumulatively the scale and effect of the harm caused to different states in order to reach the threshold of harm giving rise to self-defense.") (internal citations omitted).

[73] *See* Carly Nyst, *Interference-Based Jurisdiction Over Violations of the Right to Privacy*, EJIL: TALK! (Nov. 21, 2013), https://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/ ("In the particular case of the right to privacy, many violations are not due to extra-territorial acts, but jurisdictional acts with extra-territorial effects. That is, where interference with communications physically occurs in a particular state—the United Kingdom, for example—it can have extra-territorial effects upon those across the globe.").

[74] *See* OFF. OF THE PRESS SEC'Y, FACT SHEET: PRESIDENT XI JINPING'S STATE VISIT TO THE UNITED STATES (Sept. 25, 2015) ("The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities.") (demonstrating the U.S. and China had agreed to cooperate on the reduction of malicious cyber activities).

[75] *See* Kaelyn Lowmaster, *The US-China Cyber Agreement Matters, But It's Not Enough,* THE HILL (Oct. 18, 2017), https://thehill.com/opinion/cybersecurity/356009-the-us-china-cyber-agreement-still-matters-but-its-not-enough ("[T]his agreement won't prevent all hacks or espionage originating from China. It targets a very specific subset of intrusions—state-sponsored, targeting intellectual property, motivated by private sector benefit—and ignores other cyber issues that have since come to the fore (like cyberattacks on critical infrastructure or election tampering, for example).") (Noting that such agreements can do more, but currently leave many loopholes).

beneficiaries thereof.[76] While Sony as a corporation has little to no inherent human rights, the individuals working and affected by the Sony breach may nonetheless have a potential claim that their rights have been violated by a state actor.[77]

B. *THE DUTY TO SECURE & DUE DILIGENCE*

In contrast to general international law offering no guidance on how to secure information technology systems from foreign attackers, international human rights law provides a more proactive approach. For example, the ICCPR requires that state parties "respect and … ensure … the rights recognized in the present Covenant."[78] Similarly, the European Convention on Human Rights imposes the duty on state parties to "secure to everyone within their jurisdiction the rights and freedoms . . . ."[79] This duty has become known as the "duty to secure"[80] or the "responsibility to protect."[81] Under international human rights law, states are required not only to refrain from interfering with these rights, but also to take steps to affirmatively protect them from third-party interference.

These positive obligations have been reinforced by the Human Rights Committee in its general comments, requiring that state parties not only protect individuals from violations by state agents, but also against violations by "private persons and entities."[82] Under such interpretation, a state party may be liable for a violation of human rights even if its agents are not the ones committing the violating act,[83] if insufficient measures were enacted to ensure the enjoyment of rights.[84] This obligation to ensure enjoyment of rights is further supported by the due diligence principle, by which states are expected to

---

[76] TALLINN MANUAL, *supra* note 22, at 188 (For example, the freedom of expression may be implicated when "…the websites targeted are those of bloggers, journalists, or other individuals that disseminate information embarrassing to the State or to powerful individuals therein. . . .").

[77] *Id.* at 183 ("[I]f a hostile cyber operation is directed against the website of a human rights organisation, the customary law human rights potentially implicated are those of the organisation's members, not the organisation itself.").

[78] International Covenant on Civil and Political Rights art. 2(1), *adopted* Dec. 16, 1966, 999 U.N.T.S. 171.

[79] European Convention on Human Rights art. 1, *opened for signature* Nov. 4, 1950, Europ.T.S. No. 5, 213 U.N.T.S. 221.

[80] Yuval Shany, *Cyberspace: The Final Frontier of Extra-Territoriality in Human Rights Law* (lecture delivered in ESIL Annual Conference, Naples, Sept. 2017), https://csrcl.huji.ac.il/people/ cyberspace-final-frontier-extra-territoriality-human-rights-law.

[81] INT'L COMM'N ON INTERVENTION AND STATE SOVEREIGNTY, THE RESP. TO PROTECT (2001).

[82] Human Rights Council G.C. 31, U.N. Doc CCPR/C/21/Rev.1/Add. ("The positive obligations on State Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities. There may be circumstances in which a failure to ensure Covenant rights as required by article 2 would give rise to violations by State Parties of those rights, as a result of State Parties permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.").

[83] *See* TALLINN MANUAL, *supra* note 22, at 182 ("[I]f the activities of a non-State actor or another State interfere with the ability of individuals to engage in cyber activities protected by international human rights law, States may shoulder an obligation to ensure that the individuals entitled to benefit from the rights in question can do so.").

[84] *Id.*

undertake feasible and proportionate measures[85] to secure protected human rights.[86]

C. *BEYOND TERRITORIALITY*

International human rights law is capable of overcoming territorial constraints that often characterize general international law. As human rights are often personal, meaning they are attached to natural persons, territoriality plays no significant role.[87] Therefore, international human rights law is the right fit for a domain whose effects easily cross borders and are capable of violating fundamental human rights.[88] States would no longer be able to claim that no state territory was impacted by their operations, since the effects of these operations would be felt by individuals whose rights will certainly be implicated.

Moving beyond territoriality may be a desirable approach for the regulation of global cybersecurity, since the focus would shift from what territory or state is affected (though, not completely abandoned) to what individuals and rights are affected by an operation in cyberspace. Understandably, territoriality is a burden when translated to the cyberspace domain, as the internet may exist in multiple jurisdictions, with data flowing through multiple geographical points.[89] It exists "both everywhere and nowhere."[90]

That cyberspace undermines physical territoriality is not a novel assertion. David Johnson and David Post have previously argued that the rise of cyberspace is erasing the legitimacy of geographical-based regulation.[91] According to Johnson and Post, cyberspace "radically subverts the system of rule-making based on borders between physical spaces."[92] More recently, Jennifer Daskal referred to territoriality doctrine "in a world of highly mobile, intermingled, and divisible data" as "fiction."[93] International law's territorial foundation can therefore no longer offer an effective deterrence and remedies for violations occurring in and through cyberspace.

---

[85] *See* Human Rights Council G.C. 31, *supra* note 82, ¶ 7 (requiring that states adopt "legislative, judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations").

[86] Human Rights Council G.C. 36, U.N. Doc CCPR/C/GC/36 ("States parties are thus under a due diligence obligation to undertake reasonable positive measures, which do not impose on them impossible or disproportionate burdens, in response to foreseeable threats to life originating from private persons and entities, whose conduct is not attributable to the State.").

[87] *See* TALLINN MANUAL, *supra* note 22, at 183.

[88] *See* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370–71 (1996) ("Cyberspace has no territorially based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location. Messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another.").

[89] Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015).

[90] JOHN PERRY BARLOW, A DECLARATION OF INDEPENDENCE OF CYBERSPACE (1996) (where Barlow famously said "[o]urs is a world that is both everywhere and nowhere, but it is not where bodies live").

[91] Johnson & Post, *supra* note 88, at 1370 ("The rise of the global computer network is destroying the link between geographical location and: (1) the *power* of local governments to assert control over online behavior; (2) the *effects* of online behavior on individuals or things; (3) the *legitimacy* of a local sovereign's effort to regulate global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply.") (emphasis added).

[92] *Id.*

[93] Daskal, *supra* note 89, at 331.

III. CHALLENGES AHEAD

Conceptualizing international human rights law as a body of extraterritoriality obligations may seem outlandish for some states, the U.S. included. After all, the U.S. has resisted any interpretation of international human rights law that imposes significant obligations vis-à-vis individuals located abroad.[94] However, the same objection does not hold in an era where states are increasingly engaged in cyber operations affecting the rights of individuals abroad. States may therefore become more inclined to accept human right's extraterritoriality, considering that their own citizens are at risk of becoming victims of foreign state-sponsored cyber operations.

Even if human right's extraterritoriality gains universal acceptance and adherence, the content of the rights themselves may be unsettled and ambiguous at times, particularly when applied to cyberspace, a domain that defies territoriality, physicality, and nationality. What does the right to privacy mean in an era of ubiquitous state and corporate surveillance?[95] What are the precise contours of the right to self-determination in the wake of election hacking?[96] Further, what sort of protections from foreign interference does international human rights law afford to online speech?[97]

A. *TOWARDS POST-TERRITORIALITY*

The assertion that human rights law applies to a certain extended extraterritorially has been widely accepted throughout the international community. The European Court of Human Rights (ECtHR), for example, unanimously held that the United Kingdom had violated the European Convention for the Protection of Human Rights and Fundamental Freedoms when it failed to initiate an investigation into the deaths of five Iraqi civilians who were killed in 2003, while British forces were engaged in an operation in Basrah City.[98] The ECtHR held that when a state party "exercises effective control of an area outside that national territory" it has "the obligation to secure, in such an area, the rights and freedoms set out in the Convention."[99]

The effective control standard has indeed gained the widest acceptance among the nations.[100] However, in cyberspace, states engaging in cyber

---

[94] *See* Goodman, *supra* note 64.

[95] *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015) (proposing a framework consisting of six norms to address growing domestic and extraterritorial surveillance).

[96] *See* Michael Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 55 (2018).

[97] *See generally* Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L. J. 393 (2013).

[98] Al-Skeini and Others v. United Kingdom, App. No. 55721/07, Eur. Ct. H.R. (2011), https://hudoc.echr.coe.int/eng#{"itemid":["001-105606"]}; *see also* Wells Bennet, *The Extraterritorial Effect of Human Rights: the ECHR's Al-Skeini Decision*, LAWFARE (July 12, 2011), https://www.lawfareblog.com/extraterritorial-effect-human-rights-echrs-al-skeini-decision [hereinafter Al-Skeini].

[99] Al-Skeini, *supra* note 98.

[100] *See* Hathaway, *supra* note 11, at 2 ("All but one of the jurisdictions we examine here has articulated a test for the extraterritorial application of human rights treaties that turns on the government's 'effective control' over the territory, person, or situation in question.").

operations across borders usually lack effective control over foreign territory where the targets are residing, and therefore using the same standard of extraterritoriality would be irrelevant. Because of its ineffectiveness, it is likely that many states would feel empowered by the unrestrained legal landscape and proceed to operate in cyberspace with near impunity.

What is needed, therefore, is an extraterritoriality standard for cyberspace that takes into account the negative effects experienced by victimized individuals. While the effective control standard looks at whether a state controls territory where violations have allegedly occurred, the standard for cyberspace should equally look at whether the state has control not over territory, but over the enjoyment of rights and the effects that individuals may experience should that state decide to carry out a cyber operation.

In other words, international human rights law's extraterritoriality in cyberspace is really post-territoriality. No more should international human rights law ask whether a territory is under effective control of a foreign government, but rather whether a foreign government controls the ability of certain individuals or communities to enjoy their rights—be it the right to privacy, freedom of expression, freedom of opinion, due process, or self-determination. This approach would look at technological capacity and power, not at whether a state is in fact occupying a foreign piece of land.

This dovetails the "personal model" of extraterritoriality, where a state has physical control of an individual abroad.[101] While such a personal model is imperfect because of the prerequisite of physical control,[102] for example, when a state has "captured, arrested, or detained"[103] an individual in a foreign jurisdiction, the same personal model may be expanded to encompass technological control—the ability of states to control the enjoyment of rights not only offline, but also online, and without the use of any physical power. Moreover, new technologies of communications and data storage simply do not require the use of such physical power, making the entire analogy between physical and digital misleading.[104]

B. *THE CONTENT OF HUMAN RIGHTS*

The right to privacy, contained in Article 17(1) of the ICCPR reads: "*[n]o one shall be subjected to arbitrary or unlawful interference with his privacy.*"[105]

---

[101] *See* Eliza Watt, *The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance*, 9th INT'L CONFERENCE ON CYBER 8, 9 (2017) (noting that the personal model of extraterritoriality occurs when "state agents exercise authority and control extra-territorially . . . State agent authority is particularly pertinent in military operations where physical authority and control is exercised in formal detention centres").

[102] Rona & Aarons, *supra* note 14, at 507, 508 ("As currently defined, the spatial and personal models of extraterritorial jurisdiction and application of human rights law remain unsatisfying for application to cyberspace.").

[103] *Id.* at 508.

[104] Milanovic, *supra* note 70 ("Technological advances in obtaining information have rendered the exercise of manual, physical power over individuals unnecessary or less necessary. While privacy law in the information era frequently developed by analogy to old-school physical searches or interferences . . . there comes a point at which such analogies are no longer feasible or are outright misleading.").

[105] International Covenant on Civil and Political Rights (ICCPR), *adopted* Dec. 16, 1966, art. 17 (1), G.A. Res. 2200A (XXI), U.N. GAOR, 21st Sess., Supp. No. 16, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) (emphasis added).

But what does such a right to privacy entail when applied to cyberspace? In 1988, when the UN Human Rights Committee adopted its General Comment on the right to privacy, cyberspace "was in its infancy,"[106] and therefore the impact of new technologies on the right to privacy in the 21st century "was barely understood."[107]

The Snowden revelations have increased the calls to clarify the scope of the right to privacy in the digital era.[108] With increasing state surveillance "aggressively eavesdropping on millions of communications daily," some states have become concerned about Article 17 being outdated. That coalition of states, led by Germany, have proposed to update the right to privacy, pushing for a "globally applicable standards for data protection and the protection of privacy in accordance with the rule of law."[109]

The fear that the right to privacy is outdated, and therefore irrelevant for the digital era is understandable. Many of the human rights that are relevant to cyberspace have been enacted before most of the current information and communications technologies were in existence. The scope of these rights in the context of cyberspace was therefore never debated by the state parties involved. While it was anticipated that the same human rights would "extend to all media, regardless of new technological advancements,"[110] as of today, there is no universally accepted definition or understanding of privacy in the digital era.[111]

Similarly, there are no universal definitions or understandings for the freedom of expression, freedom of opinion, due process, and self-determination.[112] These ambiguities may undermine any idea of extraterritoriality for human rights violations in or through cyberspace. To be able to hold a violator to account, the scope of the relevant rights will need to be fleshed out through relevant state practice and the guidance of the Human Rights Council and UN General Assembly. The view held by the United States, that "development of norms for state conduct in cyberspace does not require a reinvention of customary international law,"[113] is therefore inaccurate.

C. *A HUMAN RIGHT TO CYBERSECURITY?*

The human rights currently recognized and relevant to cyberspace, namely the right to privacy, freedom of expression, freedom of opinion, due process, and self-determination, are not in themselves sufficient to address the threats posted by transnational cyber operations. If a state were to attack individual A abroad, without actually accessing any of that individual's personal data, what

---

[106] *See* Watt, *supra* note 101, at 4.

[107] *Id.*

[108] *See* Ryan Gallagher, *After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty*, SLATE (Sept. 26, 2013), https://slate.com/technology/2013/09/article-17-surveillance-update-countries-want-digital-privacy-in-the-iccpr.html.

[109] *Id.*

[110] *See* Rona & Aarons, *supra* note 14, at 505.

[111] *See* Watt, *supra* note 101, at 4, 5.

[112] *See* Ohlin, *supra* note 18, at 1596–7 (Where Ohlin identifies three substantial problems with an argument that Russian interference in the U.S. presidential election may have violated the self-determination right of American people).

[113] BARACK OBAMA, U.S. PRESIDENT, INT'L STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY AND OPENNESS IN A NETWORKED WORLD 9 (May 2011).

human rights would be implicated in such a case? The answer is that there may not be a specific right violated in this scenario. Therefore, a challenge that may arise even under a robust extraterritoriality regime is the existence of a specific right protecting an individual from state-sponsored cyber operations.

There are many ways in which cyber operations may affect individuals without implicating any existing human rights. For example, a cyber operation may target personal data belonging to an individual, but instead of viewing it, result in deletion or manipulation of that data.[114] Distributed Denial-of-Service (DDoS) may also curtail access to the internet and other valuable resources by overwhelming the target with traffic to the point of collapse.

While the right to privacy may seemingly be implicated in many of the cybersecurity incidents of recent years, this is not the case for cyber operations that are not seeking private information. The literature's focus on the right to privacy in the context of cybersecurity may be explained by the phenomenon of "privacy conflation."[115] Privacy conflation refers to the tendency to put cybersecurity in the same legal category as privacy.[116] While privacy is focused on protecting communications and deidentifying personal information, cybersecurity relates to the confidentiality, integrity, and availability ("the CIA triad") of computer systems and networks.[117] Currently, the interest reflected by the CIA triad is not fully protected by existing human rights, reinforcing the need for a specific human right to cybersecurity. For example, it is unclear whether a state interfering or manipulating encryption is in violation of the right to privacy.[118]

Aware of some of these threats, the United Nations Human Rights Council Special Rapporteur for freedom of expression has in the past urged governments to avoid cutting off access to the internet and to restore such access whenever it was cut off.[119] In other words, recognizing the importance of availability of the information and communication technologies. Along the same line, a Special Rapporteur report submitted to the Human Rights Council in 2011 notes that the internet is "acting as a catalyst for individuals to exercise their right to freedom of opinion and expression"[120] and that "the Internet also facilitates the realization of a range of other human rights."[121] It took the Human Rights Council five years

---

[114] Russell Brandom, *Everything You Need to Know About the Sony Hacks,* THE VERGE (Dec. 18, 2014), https://www.theverge.com/2014/12/18/7415735/everything-you-need-to-know-about-the-sony-hacks ("Attackers wiped every hard drive, shut down the email system, and made off with a huge cache of private company data.").

[115] *See* Matwyshyn, *supra* note 37, at 1135.

[116] *Id.*

[117] *Id.* at 1138–39.

[118] *See* Rona & Aarons, *supra* note 14, at 513 ("Human rights law is less clear about State interference with cyber-specific technologies designed to protect privacy, such as encryption. This is yet to be addressed by any international judicial body, and there is little in the way of a clear offline analog.").

[119] Office of the High Commissioner for Human Rights, *UN Expert Urges Cameroon To Restore Internet Services Cut Off In Rights Violation,* UNITED NATIONS (Feb. 10, 2017), https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21165&LangID=E ("A United Nations expert has called on the Government of Cameroon to restore internet services to predominantly English-speaking parts of the country which have been cut off in "an appalling violation of their right to freedom of expression.").

[120] UN HUM. RTS. COUNCIL, REP. OF THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION, ¶ 22, U.N. Doc. A/HRC/17/27 (May 16, 2011) [hereinafter REP. OF THE SPECIAL RAPPORTEUR].

[121] *Id.*

to pass a non-binding resolution reaffirming that "the same rights that people have offline must also be protected online,"[122] a resolution that some have framed as a recognition of basic internet access as a human right.[123]

Yet, the actions undertaken to recognize the human rights aspects of internet access do not fully capture the threat landscape and victimization of individuals in cyberspace. They are primarily addressed at states curtailing internet access to their own citizens. However, in two short paragraphs, the Special Rapporteur did recognize that state-sponsored cyberattacks, including DDoS attacks, may similarly violate the "obligation to respect the right to freedom of opinion and expression."[124] Yet, there was no mention of extraterritoriality or a human right to cybersecurity as a basis shielding individuals from state-sponsored cyberattacks. After all, if a cyberattack causes disruption that does not affect the freedom of expression of opinion, would it nonetheless be in violation of human rights obligations?

This illustrates a gap that may need resolution by the international community. In the absence of a robust human right to cybersecurity, a state may devise such carefully tailored cyber operations that seemingly do not violate any existing human right. Some calls have been made to strengthen cybersecurity globally, for example, by making "encryption of private communications" a standard.[125] While a welcomed effort, much more is needed to secure information technology systems from foreign cyber operations.

Once the need for international legal safeguards for cybersecurity is realized, it may lead to three different outcomes. First, state practice may evolve in a manner that "infuses" existing human rights with a cybersecurity flavor. In other words, an interpretive approach to existing law. Second, states may decide to enter bilateral or multilateral agreements that set out the rules and principles governing trans-border state-sponsored activities in cyberspace. Such an approach would most likely focus on the rights and duties of states, rather than individuals. Third, states may realize that an amendment to existing international human rights law is required, and that a human right to cybersecurity should be added on top of the existing human rights in various treaties and customary international law.

---

[122] UN General Assembly, *The Promotion, Protection and Enjoyment of Human Rights on The Internet*, ¶ 1, U.N. Doc. A/HRC/32/L.20 (June 27, 2016).

[123] Tim Sandle, *UN Thinks Internet Access is Human Rights,* BUS. INSIDER (July 22, 2016), https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7.

[124] REP. OF THE SPECIAL RAPPORTEUR, *supra* note 120, at ¶¶ 51–2.

[125] UN Human Rights Special Procedures, Mandate of the Special Rapporteur, *Encryption and Anonymity Follow-Up Report* at ¶ 7 (June 2018) ("Recognizing the importance of encryption to freedom of expression, privacy and related human rights, the Human Rights Council adopted a resolution in 2017 encouraging 'business enterprises to work towards enabling technical solutions to secure and protect the confidentiality of digital communications, which may include measures for encryption and anonymity.'"); Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/RES/34/7 at ¶ 9 (Apr. 7, 2017).

CONCLUSION

New technologies of information and communications challenge basic premises of existing international law, particularly because of the growing involvement and victimization of private actors, such as individuals and corporations. International human rights law may address some of the concerns overlooked by general international law, predominately through its focus on protecting individuals and private-sector entities from state-sponsored cyber operations. This Article is mindful of the fact that much more needs to be done to effectuate the full potential of international human rights law in containing the negative effects of foreign cyber operations. States and international institutions would have to further develop the doctrine of extraterritoriality in cyberspace, which ought to be supported by a more nuanced human right to cybersecurity distinguishable from the existing right to privacy and other relevant human rights.