A WAR WITHOUT BULLETS

PROTECTING CIVILIANS IN THE TECHNOLOGY TRENCHES

ABSTRACT

From probable Russian interference in the U.S. Presidential Election to the WannaCry cryptoworm, high-profile cyberattacks and cyber-intrusions of the last year have caused cybersecurity to become a topic of key political importance and a focal point of social discourse. The changing characteristics of cyberattacks, and in particular the apparent increase in nation-state involvement in such attacks, has led to a worrying shift in the nature of cyber aggression. Online hacking is no longer the preserve of the mischievous or the financially motivated, global governments are becoming increasingly active in this sphere and are using cyberattacks to pursue political objectives and national security agendas. Furthermore, as the average 21st century individual becomes progressively dependent on the Internet, he or she is growing more and more exposed to the dangers and threats posed by this reliance on the Internet. This essay addresses the legal implications of the changing trends in cyberspace. It puts forward a case for global cooperation and unifying legislation in this field, with a view to protecting civilians, in light of recent offensive use of cyber power by governments.

I. INTRODUCTION

The development of information and communication technology (ICT) has had a powerful impact on modern life. It is no exaggeration to state that few inventions have been as influential in forming our societies and economies and in determining how we interact with one another and with other parts of the globe. The move toward a digital world presents enormous benefits and potential for future growth. In recent times, we have seen the launch of self-driving cars, 3D printing, and drone-delivery options. ICT is constantly growing, and there is no indication that our progress in this field will halt any time soon. Indeed, we live in a world that is increasingly reliant on ICT and the so-called "Internet of things" (IOT). However, as our dependence on ICT amplifies, so too does our vulnerability. The daily level of cybersecurity breaches is rising, and the cost and impact of these breaches is intensifying.[1] As new areas of our lives, traditionally manually operated, become contingent on cyber activity, they open themselves up to the possibility of an attack online.

Cyberattacks are defined as "deliberate actions," seeking to

[1] *See* Kaspersky Lab, *Report: Measuring the Financial Impact of IT Security on Businesses,* 6, 9–10 (2016), https://blog.kaspersky.com/security_risks_report_financial_impact (discussing the increasing financial cost of cyberattacks for businesses); Jason Murdock, *European Commission Confirms 'Large-scale' Cyberattack Disrupted Internet for Hours*, INTERNATIONAL BUSINESS TIMES (Nov. 25, 2016), http://www.ibtimes.co.uk/european-commission-confirms-large-scale-cyberattack-disrupted-internet-hours-1593429.

"alter, disrupt, deceive, degrade or destroy computer systems or networks." [2] The IOT means that our exposure to cyberattacks now extends to physical assets that we use in everyday life, from our smart watches and household appliances, to our critical national infrastructure.[3] The Australian Red Cross and NHS Hospitals in the United Kingdom have been two of the more recent victims of such attacks.[4]

While cyberattacks can, and frequently do, target high net-worth individuals and businesses, it is clear that cyberspace is becoming the new battleground for conflicts between countries.[5] Attacks carried out by nations are no longer limited to the land, air, space or sea. The international community has recognized that a growing number of recent cyberattacks have been state-sponsored.[6] We are also seeing more governments exploit, and occasionally even weaponize, software to achieve national goals.[7] It may seem like an alarmist argument to make, but this essay queries whether a cyberwar is any less serious than a war fought on ground. When critical national infrastructure that everyday citizens rely on, such as hospitals, electricity grids, and transport networks are threatened, this is tantamount to an assault on non-combatants in times of peace. Since the late 1800s and the ratification of The Hague and Geneva Conventions,[8] the world's

---

[2] Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63, 63 (2010).

[3] *See generally* Peter J. Beshar & Tony Cole, *Cyber Risk: A Perfect Storm Approaching Europe*, BRINK NEWS (Jan. 27, 2017), http://www.brinknews.com/cyber-risk-a-perfect-storm-approaching-europe/ (explaining the "evolution of cyber risks from digital to physical assets" and the potential for attacks on national infrastructures).

[4] *EPSC Strategic Notes: Building an Effective European Cyber Shield* 1–2, EUROPEAN COMMISSION (2017).

[5] *Id.* at 1–3.

[6] *See* Howard Solomon, *Canada 'Regrets' UN Group Can't Reach Consensus on Applying International Law in Cyberspace,* IT WORLD CANADA (July 5, 2017), http://www.itworldcanada.com/article/canada-regrets-un-group-cant-reach-consensus-on-applying-international-law-in-cyberspace/394647 (discussing state-sponsored cyber-attacks).

[7] Bruce Schneier, *The NSA Is Hoarding Vulnerabilities*, SCHNEIER ON SECURITY (Aug. 26, 2016), https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html.

[8] *See* Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, July 29, 1899, Convention (X) for the Adaption to Maritime Warfare of the Principles of the Geneva Convention, Oct. 18, 1907; Convention relative to the Treatment of Prisoners of War, July 27, 1929*;* Geneva Conventions of August 12, 1949 (for the full text).

governments have been dedicated to defending civilians in times of war. Although many countries have taken legal steps in recent times to enhance cybersecurity, these measures fall short in terms of protecting civilians and in laying down a global agreement as to the parameters of acceptable online behavior of states. In short, international law is failing. This essay will explore the deficiencies in existing legislation and will make a case for a new international agreement mandating how states should behave in cyberspace.

II. THE MODERN AGE

A. Critical Infrastructure

Most major operations in the world today depend on ICT. ICT involves the integration of telecommunications (i.e., telephone lines, wireless signals, etc.) with computers, and the necessary software, storage and audio-visual systems that come with computers, thereby enabling users to access, store, transmit, and manipulate information.[9] ICT covers any product that transmits information electronically in a digital form—for example, personal computers, digital television, and GPS systems.[10]

The vast majority of infrastructure in the developed world is completely reliant on ICT.[11] Industrial control systems (ICS) and supervisory control and data acquisition systems (SCADA) are utilized throughout infrastructure systems across the world in water, electricity, gas, petroleum, pipelines, and transport.[12] ICS and SCADA are the building blocks of automated systems where control or monitoring of a process is required.[13] Essentially, in order for citizens to access vital utilities, ICT must be running smoothly.[14] The Department of Homeland Security in the United States defines critical national infrastructure as the "assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have

---

[9] Shariful Islam & Nazmul Islam, *Information and Communication Techno logy (ICT) in Libraries: A New Dimension in Librarianship*, 5(8) ASIAN J. INFO. TECH. 809, 809 (2006).

[10] *Id.*

[11] Stephan Gottwald, *Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure* 7 (2009).

[12] Keith Stouffer et al., *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, NAT'L INST. OF STANDARDS & TECH. 2–1 (2006).

[13] *Id.*

[14] *See id.* (explaining how vital utilities are operated by ICT)

a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[15] Similarly, the E.U. defines critical infrastructure as:

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[16]

As ICT continues to develop and as modern society's dependence on the Internet deepens, it is important to bear in mind that these definitions of critical infrastructure will likely expand to encompass the equipment and apparatus underpinning everyday life.

Due to our increasing reliance on ICT, the functioning of critical infrastructure across the globe has become contingent on a high-level of assured cybersecurity. In connection with this, politically driven governments and cyber attackers with geostrategic concerns, are turning their attention to critical national infrastructure.

B. Cyberattacks on Critical Infrastructure

This area has become a key focus point for online attackers in recent times, particularly because the potential to destabilize rival countries and cause vast amounts of harm is so great.[17] Cyberattacks on critical infrastructure have been steadily growing in both the U.S. and in Europe.[18] These attacks are markedly lethal as they represent a unique ability to combine online threats with on-ground operations.[19] In the Russo-Georgian War of 2008, Georgia accused Russia of combining cyberattacks with traditional

---

[15] *What is Critical Infrastructure?* U.S. DEP'T OF HOMELAND SEC. (July 12, 2017), https://www.dhs.gov/what-critical-infrastructure.

[16] Council Directive 2008/114/EC at Art. 2(a), 2008 O.J. (L 345) (EC).

[17] *See* Bret Brasso, *Cyber Attacks Against Critical Infrastructure are No Longer Just Theories*, FIREEYE (Apr. 29, 2016), https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html (discussing the increasing amount of cyberattacks and the devastation they cause).

[18] Andrew Meola, *Cyber Attacks Against Our Critical Infrastructure are Likely to Increase*, BUSINESS INSIDER (May 26, 2016), http://uk.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5?r=US&IR=T.

[19] *See Georgian Cyber Attack (2008) in* ENCYCLOPEDIA OF CYBER WARFARE 119 (Paul J. Springer ed., 2017) (discussing Russia's use of ground attacks with cyber attacks).

military operations.[20] The New York Times reported that this marked the first time in history that a cyberattack had supplemented a shooting war.[21] The effects were devastating.[22] Russia completely thwarted the capabilities of Georgian military personnel during a time of great panic and confusion.[23] Both Poland and Estonia offered online assistance to Georgia, and the President of Poland, Lech Kaczynski, stated that he would grant Georgia access to the official website of the Republic of Poland so that Georgian officials could disseminate information.[24] This is an example of how a cyberattack on one nation-state can spiral into a situation involving neighboring countries and allies.

The incidence of such state-sponsored cyberattacks is escalating.[25] Germany openly accused Russia of involvement in the 2015 attack on its parliament, the Bundestag.[26] More recently, members of the U.S. government have stated that the 2016 cyberattack on the U.S. Democratic National Committee was the work of Russian intelligence agencies.[27] While Russia appears to be the main player currently engaging in this activity, we know that North Korea, China, and the U.S. have also implemented cyberattacks in recent years; it is only a matter of time before the practice becomes even more widespread among nation-states.[28]

Politically motivated cyberattacks are gaining in hostility and complexity.[29] Such attacks might serve a legitimate purpose as

---

[20] Tom Espiner, *Georgia accuses Russia of coordinated cyberattack,* CNET (Aug. 12, 2008), https://www.cnet.com/au/news/georgia-accuses-russia-of-coordinated-cyberattack/.

[21] John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[22] *See* Espiner, *supra* note 20 (discussing effects of the cyberattack).

[23] *Id.*

[24] *Id*.

[25] *See* Julie Cohn, *Is Your Business Ready for Cyber War?* NBC NEWS (Feb. 14, 2013), http://www.nbcnews.com/id/50809654/ns/business-small_business/ (advising businesses to bolster their cybersecurity).

[26] Jay Greenberg, *Germany Accuses Russia of Attempting to Hack German Elections,* NEON NETTLE (July 4, 2017), http://www.neonnettle.com/news/2357-germany-accuses-russia-of-attempting-to-hack-german-elections.

[27] Spencer Ackerman & Sam Thielman, *US Officially Accuses Russia of Hacking DNC and Interfering with Election*, THE GUARDIAN (Oct. 8, 2016), https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election.

[28] *See* Oona A. Hathaway et al., *The Law of Cyber-Attack,* 100 CALIF. L. REV 817, 820, 838 (2012) (discussing evidence of China's involvement in cyber warfare, plus the likelihood of involvement by the U.S., Russia, and North Korea).

[29] *See* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV 1533, 1538–39 (2010).

part of a targeted military campaign, but as it currently stands, certain nation-states are using them in an abusive and arbitrary manner.[30] Without any kind of binding global agreement governing the use of cyber force by states, these attacks risk undermining the operation of Western democracies. When U.S. government officials announced that Russia likely interfered in the U.S. election using cyberattacks, certain members of the public reacted with outrage and participated in protests.[31] One website even began selling "Trump elected by Russia" T-shirts.[32] In a comment that might be judged as dramatic, but that serves to illustrate the current lack of faith and trust in our systems, one member of Congress remarked that, "We might as well mail our ballot boxes to Russia."[33] Western democracy is premised on the idea that citizens exercise power over their own affairs. In every modern society, whether based on democratic values or not, critical infrastructure is the crucial machinery that citizens depend on for their most basic needs.[34] Accordingly, I would contend that the age-old adage of, "all is fair in love and war" should not apply to these areas. Nation-states have a duty to come together and ensure that robust systems of protection are in place. Otherwise, there is a real risk that we will descend into a world where one of our greatest creations, the Internet, becomes our undoing - our very own 21st century Frankenstein monster.

Russia's recent cyberattacks on the Ukrainian electricity grid depict a menacing picture of what the future might look like if the world's governments do not come together and regulate the use of cyberattacks by state actors.[35] These attacks, which occurred in

---

[30] Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties in* FROM THE SELECTED WORKS OF SUSAN BRENNER 4 (2010) (explaining how civilians can become causalities in cyberwarfare because nation-states use civilians as a means of attacking others)

[31] Amanda Terkel, *Bipartisan Anger Grows Over Russian Interference into U.S. Election,* THE HUFFINGTON POST (Dec. 11, 2016), https://www.huffingtonpost.com/entry/russian-hacking-trump_us_584d7403e4b04c8e2bb04591.

[32] *Donald Trump – Elected by Russia*, TEESPRING, https://teespring.com/shop/trump-elected-by-russia#pid=2&cid=2122&sid=front.

[33] Jennifer Van Laar, *Adam Schiff: "We Might as well Mail our Ballot Boxes to Russia,"* TOWNHALL (July 9, 2017), https://townhall.com/tipsheet/jennifervanlaar/2017/07/09/adam-schiff-we-might-as-well-mail-our-ballot-boxes-to-russia-n2352489.

[34] *See Role of Critical Infrastructure in National Prosperity* in CRITICAL 5 (2015) (discussing why critical infrastructure is crucial for national prosperity).

[35] *See* Andy Greenburg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017), https://www.wired.com/story/russian-hackers-attack-ukraine/ (explaining how, because of Russia's technological advancements

both 2015 and 2016, represented a dangerous flexing of Russia's muscle.[36] They targeted a neighboring country and manipulated a system of its critical national infrastructure for no apparent reason, other than to signal their strength and their ability to cause havoc.[37] Pavel Polityuk reported that the outage amounted to 200 megawatts of capacity, equivalent to about a fifth of Kiev's energy consumption at night.[38] Ukrainian civilians suffered a number of adverse effects following this unprovoked act of aggression.[39] Nation-states can no longer afford to sit idly by.

C. Why now?

The international community cannot deny that the rate at which cyberattacks are increasing, coupled with the worrying progression of state involvement, means that we are on the cusp of a cyberwar.[40] Recent attacks have been of such a degree that they could arguably fall within Article 5 of the North Atlantic Treaty 1949 (the NATO Treaty) or Article 51 of the Charter of the United Nations 1945 (the UN Charter). Article 5 of the NATO Treaty states that:

> [a]n armed attack against one or more of [the parties to the Treaty] shall be considered an attack against them all and consequently [. . .] if such an armed attack occurs, each of them [. . .] will assist the Party or Parties so attacked by taking [. . .] such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[41]

NATO has committed to increasing cyber defense.[42] At the Wales

---

cyberwarfare is now a reality).

[36] *See id.* (showing that there have been cyberattacks in the Ukraine throughout the past three years).

[37] *See EPSC Strategic Notes*, *supra* note 4, at 3 (explaining how cyberattacks are being used to experiment regarding the level of damage they can cause).

[38] Pavel Polityuk, *Ukraine Investigates Suspected Cyber Attack on Kiev Power Grid*, REUTERS (Dec. 20, 2016), http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF.

[39] *See* Lizzie Dearden, *Ukraine Cyber Attack: Chaos as National Bank, State Power Provider and Airport Hit by Hackers*, THE INDEPENDENT (June 27, 2017), http://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html (discussing various effects on Ukrainian citizens, including the postal service, television stations, transport, ATMs, and banks being down or inaccessible).

[40] *See id.* (explaining that cyberattacks have drastically increased).

[41] North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243.

[42] *See* Ryan Brown, *NATO: We Ward Off 500 Cyberattacks Each Month*, CNN (July 18, 2017), http://www.cnn.com/2017/01/19/politics/nato-500-cyberattacks-

Summit, in September 2014, it formally recognized cyberspace as an area of military operation, meaning that a party to the NATO Treaty may now potentially invoke Article 5 following a cyberattack, if the cyberattack is serious enough to constitute an armed attack.[43] Considering the scale of recent cyberattacks, that time might not be far-off unless we take drastic action soon.

Article 51 of the U.N. Charter contains similar language and provides that, "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence [sic] if an armed attack occurs against a Member of the United Nations."[44] The risk of cyberattacks cascading into global panic affecting numerous countries is becoming palpable. The nations of the world must work as one and put preventive measures in place to deter such cyberattacks, or at the very least determine the circumstances in which they may be used.

A number of stark statistics support this call for action. Over 315 million Europeans use the Internet on a daily basis.[45] In these fraught times, that figure translates to 315 million online civilians at risk in Europe alone. This figure extends beyond the online sphere when we take account of the fact that an online attack can have consequences on the ground as well—for example, where a traffic light system is hacked. As it stands, critical national infrastructure and communication systems are suffering from attacks on a daily basis.[46] The level of these attacks and the damage caused by them is also increasing.[47] The World Economic Forum Global Risks Report for 2017 ranked technological risks, most notably cyberattacks, among the most likely and most impactful global risks.[48] Governmental experts speculate that the use of cyberattacks between states is "becoming more likely" and that the risk of "attacks against critical infrastructure is both real

---

monthly/index.html.

[43] *See* discussion *infra* Part II (on classifying cyberattacks).

[44] U.N. Charter art. 51.

[45] *State of the Union 2016: Commission Paves the Way for More and Better Internet Connectivity for all Citizens and Businesses*, EUROPEAN COMMISSION (Sept. 14, 2016), http://europa.eu/rapid/press-release_MEMO-16-3009_en.htm.

[46] *Critical Infrastructure and Communications Security*, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/general/critical-infrastructure-and-communications-security.

[47] Angela Messer & Brad Medairy, *Industrial Cybersecurity Threats Are on the Rise*, BOOZ ALLEN HAMILTON, https://www.boozallen.com/s/insight/thought-leadership/industrial-cybersecurity-threats-are-on-the-rise.html.

[48] *Global Risks Report 2017*, WORLD ECONOMIC FORUM (12th ed.).

and serious."[49]

In addition, the cost of dealing with and remedying the fallout from these attacks is rising astronomically. According to a UK Government report, 90% of large UK firms experienced an attack in 2015, versus 81% in 2014, and the costs in connection with this climbed from £1.15m in 2014 to £3.14m in 2015.[50] Another report published in August 2016 by the European Network and Information Security Agency (ENISA) stated that losses accumulated through cyberattacks amounted to 1.6% of GDP in some E.U. countries.[51] Recent studies indicate that the situation is only set to worsen, with one report suggesting that the cost of damage caused by cyberattacks will quadruple in the next two years, reaching $2 trillion worldwide by 2019.[52]

III. WHEN DOES A CYBERATTACK BECOME A CYBERWAR?

Given the global nature of the Internet, many cyberattacks and cybersecurity incidents transcend national borders and have the potential to undermine international security generally.[53] But when does a cyberattack become a war? Characterizing war has always been a problematic concept. In the past, the initiation of combat simply hinged on a formal declaration of war by a state. No strict rules were in place, and there was no legal framework governing the process.[54] That is no longer the case; international law has moved away from the historical concept of war and has replaced the notion with a number of complex and strict legal rules.[55] World War II and the mass destruction that came with it led to the development of the U.N. Charter, which sets out the

---

[49] SECRETARY-GENERAL, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 4–5, U.N. Doc. A/70/174 (July 22, 2015).

[50] PRICEWATERHOUSECOOPERS, 2015 INFORMATION SECURITY BREACHES SURVEY

[51] DAN TOFAN ET AL., THE COST OF INCIDENTS AFFECTING CIIS 04 (E.U. Agency for Network and Information Security, 2016)

[52] *Cybercrime Will Cost Businesses Over $2 Trillion by 2019*, JUNIPER RESEARCH (May 12, 2015), https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

[53] Derek Reveron, *How Cyberspace is Transforming International Security,* HARVARD UNIVERSITY, https://www.extension.harvard.edu/inside-extension/how-cyberspace-transforming-international-security.

[54] Jennifer K. Elsea & Matthew C. Weed, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications*, CONGRESSIONAL RESEARCH SERVICE (2014).

[55] *See* Harold H. Koh, *Why Do Nations Obey International Law?* 106 YALE L.J. 2599, 2599–2601 (1997) (for discussion of the evolution of international law).

criteria and the circumstances in which nation-states may use force.[56]

Article 2(4) of the U.N. Charter provides that, "[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[57] This prohibition on the use of force against another state represents customary international law and is a generally accepted principle of law.[58] However, Article 51 of the U.N. Charter states that where a nation-state has suffered an armed attack, it may resort to self-defense.[59] When read in tandem, these articles raise two fundamental questions: (1) what constitutes a use of force; and (2) what is an armed attack? Furthermore, can the launch of a cyberattack by a state against another state be such that it constitutes the use of force taking the form of an armed attack? If so, when such an attack occurs, can the victim-state have recourse to self-defense and rely on Article 51?

The U.N. Charter is silent as to what forms the use of force, in the context of Article 2(4), might take.[60] While the drafters of the U.N. Charter would likely not have had cyberattacks on their radar in the mid-1940s, it is clear that the Article provides a level of flexibility in its broad use of terms. When considering what might amount to a use of force, nation-states frequently have regard to the consequences suffered as well as the instrument used to apply the force. As there is no "internationally accepted consensus on a precise definition of use of force, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[61] Similarly, there is no concrete definition of an "armed attack."[62] The *Nicaragua* case is authority for the principle that all "all armed attacks are uses of force, but not all uses of force qualify as armed attacks."[63] Michael

---

[56] U.N. Charter art. 2 ¶ 3–5.

[57] *Id.* at ¶ 4.

[58] *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 187–91 (June 27) (discussing the support for the principle of non-aggression in international relations).

[59] U.N. Charter art. 51.

[60] *See id.* at art. 2, ¶ 4 (failing to provide a definition of "use of force").

[61] *Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm.,* 111th Cong. 11 (2010).

[62] *See id.* at 12 (suggesting that the definition of "armed attack" is subjective).

[63] Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts, in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND

N. Schmitt states that, "[t]he essence of an armed operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects."[64] The Tallinn Manual on the International Law Applicable to Cyber Warfare provides that, "whether a cyber-operation constitutes an armed attack depends on its scale and effects."[65] The group of legal experts behind the manual agreed that an armed attack does not necessarily involve the use of traditional "weapons."[66] If the results of a cyberattack are equivalent to those caused by a traditional military operation, the instrument used to cause the effects is not important. [67] The Red Cross considers that a weapon is a "means to commit acts of violence."[68] Clearly, cyber tools can meet that definition.

A number of states are beginning to agree that cyber weapons are "just another weapons system, cheaper and faster than a missile, [and] potentially more covert."[69] When states use cyber weapons as a means of attack to target critical infrastructure and property, they inadvertently attack the people relying on those systems and this activity must be seen as a use of force falling within the reach of Article 2(4).[70] Furthermore, if this use of force causes a high level of damage, it should be viewed as an armed attack. We can no longer afford to classify war and weaponry in archaic and outdated terms. To continue to do so will leave online civilians exposed. Not only that, but it also means that citizens on the ground will be subject to the real-life effects of virtual attacks and their governments will not be in a position to protect them.

Take the recent example of the Ukraine, left without electricity when their power grid was hacked by a neighboring state in an

---

DEVELOPING OPTIONS FOR U.S. POLICY 151, 163 (Nat'l Acad. Press ed., 2010).

[64] *Id.*

[65] TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 54 (Michael N. Schmitt ed., 2013).

[66] *Id.* at 55.

[67] See *id.* (stating the "critical factor" for determining whether an operation qualified as an "armed attack").

[68] JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: VOLUME I 23 (Cambridge Univ. Press ed., 2005).

[69] James Lewis, *To Protect the U.S. Against Cyberwar, Best Defense is a Good Offense,* U.S. NEWS AND WORLD REPORT (Mar. 29, 2010), http://www.usnews.com/opinion/articles/2010/03/29/to-protect-the-us-against-cyberwar-best-defense-is-a-good-offense.

[70] Daniel B. Silver, *Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter*, 76 INT'L L. STUD. 91, 92–93 (2002).

unprovoked act of force.[71] The lack of clear definitions around this type of cyber activity and the dearth of rules to abide by means that it is a free for all. The resultant confusion allows certain cyber-strong nations to exert force without consequences, all to the harm of the civilian. While the power outages may not have led to any deaths or lasting physical damage, it is clear that they had the capacity to do so. It does not take much imagination to think about how the consequences could have been even more severe if air-traffic control, for example, had been hacked. More importantly, the attacks profoundly disrupted the functioning of Ukrainian society.[72]

This most recent attack on the Ukraine is just the latest in what is now a rapidly mounting list of cyberattacks carried out by nation-states.[73] It is widely suspected that Russia was behind recent similar attacks in Estonia and Georgia.[74] From 2005 to 2012, the U.S. and Israel worked together to develop Stuxnet, which eventually sabotaged Iranian nuclear facilities.[75] And after extensive investigation, experts linked the recent cyberattack on Sony Pictures to North Korea.[76] Not only is a trend emerging, it is multiplying.

One commentator in this field declared that cyberattacks have been, "the most influential instrument of the past two decades."[77] In spite of this, international law has failed to recognize the use of cyberattacks as a weapon of national strategy in any legally binding text.[78] Currently, the criteria for assessing violations of the NATO Treaty and the U.N. Charter, in a cyberspace context,

---

[71] Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[72] *See id.* (for discussion of the effects of the attack).

[73] Tara Seals, *Cyber-attack Volume Doubled in First Half of 2017*, INFOSECURITY MAGAZINE (Aug. 11, 2017), https://www.infosecurity-magazine.com/news/cyberattack-volume-doubled-2017/.

[74] *See* John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

[75] Adeo Fraser, *From the Kalashnikov to the Keyboard: International Law's Failure to Define a 'Cyber Use of Force' is Dangerous and May Lead to a Military Response to a 'Cyber Use of Force,'* 15 HIBERNIAN L.J. 86, 95 (2016).

[76] David E. Sanger & Nicole Perlroth, *U.S. Said to Find North Korea Ordered Cyberattack on Sony*, NEW YORK TIMES (Dec. 17, 2014), https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

[77] FRED SCHREIER, DCAF HORIZON 2015 WORKING PAPER NO. 7: ON CYBERWARFARE 16 (2015).

[78] Oona A. Hathaway & Rebecca Crootof, *The Law of Cyber-Attack*, YALE L. SCH. 817, 846 (2012).

are imprecise. Admittedly, online attacks strain the conventional understandings of armed conflict. However, leaks of sensitive data, attacks on critical infrastructure and interference in the democratic processes of Western society mean that cyberwar is no longer a dystopian, future threat. It is a reality. Moreover, the time is ripe for the international community to re-visit its laws.

IV. THE CURRENT LEGAL FRAMEWORK AND ITS SHORTCOMINGS

It is not a novel idea to propose legislation that would tackle damage caused over the Internet.[79] Since the 1990s, many states have implemented Internet laws.[80] There have even been some international conventions, treaties, and directives seeking to control cross-border harms caused by cyber operations.[81] Yet, none of these goes far enough. The bulk of existing legislation concerns non-state actors and is limited to the private sphere.[82]

A. The Budapest Convention

The 2001 Budapest Convention on Cybercrime (the Budapest Convention)[83] established a "common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation."[84] It required the parties thereto to adopt national laws banning a number of computer crimes, from data and system interference to misuse of devices.[85] This proved unsatisfactory, however, as it led to a fragmented scenario where the national laws adopted by each

---

[79] Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, HOOVER INSTITUTION 3, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.

[80] *See State Laws Related to Internet Privacy*, NAT'L CONF. OF ST. LEGISLATURES (June 20, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx (for some of the states and citations to their respective Internet privacy laws).

[81] *See Cybersecurity: A Global Issue Demanding a Global Approach*, U.N. DESA (Dec. 12, 2011), http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html (discussing a U.N. cybersecurity special event).

[82] *See* SCHREIER, *supra* note 77 (describing needs for existing legislation to grow beyond its current representation of non-state actors and the private sector).

[83] Council of Europe Convention on Cybercrime, The Budapest Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. No. 185.

[84] *Id.*

[85] *See id.* (laying out the need for an adoption of laws that will allow for combating cybercriminal offenses).

signatory differed greatly in their interpretation and scope.[86] Furthermore, many large nations with strong cyber capabilities have not ratified the Budapest Convention, including the United Kingdom and Russia.[87] Crucially, the Budapest Convention does not apply to inter-state cyber operations; rather it applies to private persons undertaking internet activity in signatory states.[88]

B. Sino-U.S. Cybersecurity Agreement

In September 2015, the president of China, Xi Jinping, visited the White House.[89] During this visit, President Xi Jinping and President Obama reached agreement on a number of issues.[90] Among these were a number of pledges related to cybersecurity.[91] The two heads of state agreed to cooperate with one another and provide information on malicious cyber activities and cybercrimes.[92] They further committed that neither country's government would conduct or knowingly support cyber-theft of intellectual property or confidential information.[93] The agreement was largely limited to business matters and commercial interests.[94] Notably, it does not extend to national security issues.[95] Nevertheless, both leaders did express a desire to classify appropriate norms of state behavior in cyberspace in the future.[96]

---

[86] *See* Joyce Hakmeh, *Building a Stronger International Legal Framework on Cybercrime,* CHATHAM HOUSE (June 6, 2017), https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime# (addressing the imperfect nature of the Budapest Convention).

[87] *Id.*

[88] *See generally* Budapest Convention, *supra* note 83 (for discussion of its scope).

[89] Gary Brown & Christopher D. Yung, *Evaluating the U.S.-China Cybersecurity Agreement, Part 1: The U.S. Approach to Cyberspace,* THE DIPLOMAT (Jan. 19, 2017), http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1/.

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] *Id.*

[94] *See id.* (addressing commercial interests the U.S. and China seek to protect).

[95] Gary Brown & Christopher D. Yung, *Evaluating the U.S.-China Cybersecurity Agreement, Part 3: China's Take on Cyberspace and Cybersecurity,* THE DIPLOMAT (Jan. 21, 2017), https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/.

[96] Everett Rosenfeld, *U.S.-China Agree to Not Conduct Cybertheft of Intellectual Property,* CNBC (Sept. 25, 2015), https://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

There have been allegations that this agreement means very little to China and that hackers based in China have continued to engage in cyber operations against U.S. systems.[97] Even if this is the case, and if China is continuing its cyber espionage and attacks, this does not render the agreement a failure. In entering the agreement, China has formally recognized that there are areas of prohibited cyber activity and the U.S. now has a prescribed framework to point to should it deem that China has breached its commitments. The agreement places pressure on China and encourages adherence to the law regarding conduct in cyberspace, not least because it paves the way for economic sanctions and public naming-and-shaming if breaches occur.[98]

C. G20 Leaders' Communiqué, Antalya Summit, November 2015

Just two months after the meeting between President Obama and President Xi Jinping, the world's leaders made similar commitments at the G20 summit.[99] For the first time, the global community acknowledged publicly that states have a responsibility to promote inter-state security and stability in a cybersecurity context.[100] The countries of the world stated that they hoped to "bridge the digital divide."[101] However, like the U.S. and China, they limited their specific agreement to commercial concerns, such as intellectual property, trade secrets, and confidential business information.[102] They stated that they would not use cyber operations to interfere in these areas with the intent of providing competitive advantages to companies or commercial sectors.[103] The leaders also informally affirmed that international law, and in particular the U.N. Charter, is applicable to state

---

[97] *U.S.-China Part 3*, *supra* note 95.

[98] Ellen Nakashima & Steven Mufson, *U.S., China Vow Not to Engage in Economic Cyberespionage*, THE WASHINGTON POST (Sept. 25, 2015), https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html?utm_term=.b1cf3a720b35.

[99] *FACT SHEET: The 2015 G-20 Summit in Antalya, Turkey,* WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Nov. 16, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/11/16/fact-sheet-2015-g-20-summit-antalya-turkey.

[100] *Id.*

[101] *G20 Leaders' Communiqué Agreed in Antalya* ¶ 26, G20 (Nov. 15-16, 2005), http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/.

[102] *Id.*

[103] *Id.*

conduct in the use of ICT.[104] They expressed that they were "committed to the view that all states should abide by norms of responsible state behaviour in the use of ICTs."[105] This represents a very positive step in the right direction, but the world's governments now need to expand upon this affirmation in a binding global treaty that sets out clear principles and rules of state activity in cyber space.

D. NIS Directive

Perhaps the most prescriptive piece of legislation to date in this area is the 2016 E.U. Directive on Security of Network and Information Systems (the NIS Directive).[106] The NIS Directive's principal aim is to enhance the security of systems that rely on ICT.[107] It requires that providers of essential services have in place appropriate technical and organizational measures to protect the security of their systems and to protect strategic essential infrastructure in fields such as electricity, gas, water, and transport from cyberattacks.[108] Failure to comply with certain terms set out in the NIS Directive may lead to fines of up to €10m or 2% of the provider's global turnover.[109] The NIS Directive builds on existing measures under the 2008 European Critical Infrastructure Directive[110] (the 2008 Directive) and the 2013 Cybercrime Directive[111] (the 2013 Directive). The 2008 Directive required E.U. member-states to identify critical infrastructure in their energy and transport sectors and to establish a coordinated security approach to that infrastructure through the appointment of so-called Security Liaison Officers.[112] The 2013 Directive aimed to tackle large-scale cyberattacks by requiring E.U. member-states to strengthen national cybercrime laws and introduce tougher criminal sanctions.[113]

The NIS Directive has arguably gone further than any piece of law before it. At its core, it seeks to protect critical infrastructure,

---

104 *Id.*
105 *Id.*
106 Directive 2016/1148, 2016 O.J. (L 194) 1 (EC).
107 *Id.* at ¶ 8.
108 Directive 2016/1148, *supra* note 106, at ¶ 34, Annex II.
109 Directive 2016/679 at Art. 83(4), 2016 O.J. (L 119) 1 (EC).
110 *See* Council Directive 2008/114, *supra* note 16 (for the 2008 Directive).
111 *See* Directive 2013/40, 2013 O.J. (L 218) 8 (EC) (for the 2013 Directive).
112 Council Directive 2008/114, *supra* note 16, at ¶ 12.
113 Council Directive 2013/40, *supra* note 111, at Art. 10–11.

and it places a number of obligations on private operators.[114] These private operators must put state-of-the-art security measures in place, and they must report cyberattacks when they occur.[115] The reporting of cyberattacks aims to promote increased transparency and knowledge sharing among E.U. member-states.[116] A key provision is set out in Article 15 of the NIS Directive, and this provides that the E.U. Commission may issue binding instructions on private operators to update and improve their security systems if they are not satisfied with the systems currently in place.[117] If implemented correctly, the NIS Directive will do a great deal to raise the common baseline of cybersecurity in the E.U.[118] It deserves credit on those grounds alone. Yet, it still fails to hit the mark required. It only speaks to non-state actors, and it provides no guidance as to how nation-states should behave in terms of their online conduct.[119] Furthermore, as it is an E.U. Directive, it excludes a number of important non-E.U. nation-states.

E. International Law

International law is purportedly applicable and vital to the maintenance of stability in cyberspace.[120] Perversely, however, this very essential and applicable body of law predates that which it is supposed to govern. How can we seek to apply the Geneva Convention and the U.N. Charter to cyberattacks, when they never envisaged such a type of warfare? Furthermore, while there is some evidence that the U.N. Charter has expanded to include cyberattacks in "use of force" and even in "armed force,"[121] and while many commentators have put forth strong arguments that this is the case,[122] the question is far from settled. Adeo Fraser

---

[114] *See generally* Directive 2016/1148, *supra* note 106 (for the full text of the Directive).

[115] *Id.* at ¶ 4, 10.

[116] *Id.* at ¶ 36.

[117] *Id.* at Art. 15(3).

[118] *See generally id.* (for the full requirements of the Directive).

[119] *See generally id.* (for scope of the Directive).

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

[121] *See G20 Leaders' Communiqué*, *supra* note 101 (discussing the applicability of the U.N. Charter to cyberspace).

[122] *See* Schmitt, *supra* note 63 (arguing that cyberattacks constitute a use of force); *see also* Knut Dörmann, *Applicability of Additional Protocols to Computer Network Attacks*, INT'L COMMITTEE RED CROSS (Nov. 19, 2004), https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.

favors a narrow interpretation of the U.N. Charter.[123] Others go further still and stipulate that Article 2(4) of the U.N. Charter and its reference to "use of force" means "armed force" only.[124] However, I would draw attention to the fact that in many other articles of the U.N. Charter, the drafters used the term "armed force."[125] If the U.N. intended to limit Article 2(4) in this fashion, surely it would have availed of the term "armed force," as opposed to the looser term "use of force." The maxim *expressio unius est exclusio alterius* comes into play here. When Article 2(4) is examined using that lens, it would seem to me that not only is there sufficient scope in Article 2(4) to include cyberattacks in its remit, but that there was also a clear intention that the understanding of use of force was not to be limited to armed force or traditional armed attacks. In any event, and as explained above, there is room for argument that a cyberattack can be an armed attack if sufficiently serious. Nevertheless, it is important to concede that the use of cyberattacks and cyber force as a form of armed attack has not been formally accepted in any binding or effective framework that international law can regulate.[126] Furthermore, the ongoing academic debate on the scope of Article 2(4) and the lack of domain specific clarity is only exacerbating the confusion in this field. While many countries have informally recognized that the law of armed conflict and the law on the use of force applies to cyber operations,[127] we need to ask ourselves if a system based on informal and loose cooperation between nation-states will suffice to make the world cyber-secure. It is hard to see how we could have faith that this will be the case. Where there is imprecision and where there are gaps in definitions, those who seek to do harm to rival nations and those who wish to inflict damage on infrastructure, using cyberattacks, will do so by occupying those vague regions and by availing of the flexibility that the gaps provide.

---

123 Fraser, *supra* note 75, at 91.

124 *See* Albrecht Randelzhofer and Oliver Dörr, *Article 2*, *in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 129 (Bruno Simma et al. eds., 3rd ed. 2002).

125 *See, e.g.*, U.N. Charter art. 41, 46 (for two provisions that use "armed force").

126 *See* Fraser, *supra* note 75, at 89 (explaining the lack of a law in which cyber force is defined as an armed attack).

127 MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 19–21 (Oxford U. Press, 2014).

V. CASE FOR NEW LAW

What we need now is a global convention that will define cyber force and cyber terminology, and that will set down precise rules governing inter-state cyber activity.[128] The current legal framework is inadequate. Clear gaps exist in international law regarding defined terms and how the world's governments should behave in cyberspace. The U.N. Charter, the NATO Treaty and the Geneva Conventions are silent on the question of cyberattacks, their drafting having largely predated cyber operations. However, just as the law evolved to outlaw the use of chemical weapons against civilians, as such weapons were developed and being seen in use,[129] so too must the law now proceed to ban cyberattacks against critical civilian infrastructure such as hospitals and national energy systems.

Despite this need for change, we do not need to revise the U.N. Charter. It adequately addresses traditional inter-state combat and use of force, which is what it intended to capture. Rather than attempting to wedge cyberattacks into this regime, we should implement a new framework, purposely designed to address state use of cyber force. What we need now is a U.N. Cyber Charter. By creating a new and separate U.N. Cyber Charter, we would be leaving space for flexibility and for expansion on the new principles set out therein, whereas if we were to revisit and amend the existing U.N. Charter, as Schmitt proposes,[130] we would have to make as little changes as possible so as not to do harm to the underlying text and principles on which the U.N. Charter is founded.

Demands for an international treaty regulating cyber force are not new. The Russians have been advocating for a cyberwarfare treaty for years.[131] Stanford University's Center for International Security and Cooperation published the first formal recommendation in the U.S. for a multilateral treaty to deal with

---

[128] Brad Smith, President, Microsoft Corp., Keynote Address at the RSA Conference 2017: The Need for a Digital Geneva Convention (Feb. 14, 2017) (transcript available at https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf).

[129] *Id.*

[130] *See* Schmitt *supra* note 63, at 178 (for Schmitt's discussion on the point).

[131] CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cybercom (June 3, 2010) (transcript available at https://fedgeno.com/documents/us-cybersecurity-policy-and-the-role-of-the-us-cybercom.pdf).

cybersecurity in 2000.[132] They proposed creating an international regulatory agency that would rely on expert private assistance.[133] More recently, in February 2017, the President of Microsoft, Brad Smith, renewed calls for an international treaty on cybersecurity.[134] Unfortunately, putting a treaty to paper has met a great deal of resistance to date.[135] Following the G20 summit in Hamburg in July 2017, President Trump announced that he and President Putin were looking into forming an "impenetrable cybersecurity unit."[136] Many commentators criticized President Trump's announcement and branded it as akin to having the henhouse guarded by the fox.[137] Following such criticisms, President Trump immediately retreated on the plan, even though some specialists in the area felt that it could have its merits if carefully considered.[138] A joint cybersecurity unit may well not be a wise decision and the detractors who would resist sharing information and state secrets are right to be concerned. However, that is not to say that we should not cooperate with other nations or strive to reach agreement on less contentious issues, such as pledges not to attack critical infrastructure.

Schmitt remarks that we are unlikely to see any meaningful treaty negotiated in the near future.[139] He points to the fact that the countries that are most vulnerable to cyberattack are also those most capable of conducting them.[140] Consequently, nation-states will be hesitant to limit their freedom of action.[141] This is no doubt a valid argument. The recent example of certain nation-states' behavior in the context of the U.N. treaty on the prohibition

---

132 ABRAHAM D. SOFAER ET AL., A PROPOSAL FOR AN INTERNATIONAL CONVENTION ON CYBER CRIME AND TERRORISM i–ii (2000).

133 *Id*. at iv.

134 Smith, *supra* note 128.

135 *See* Kenneth Corbin, *State Department Argues Against 'Cyber Arms' Treaty*, CIO (May 26, 2016), https://www.cio.com/article/3075442/government/state-department-argues-against-cyber-arms-treaty.html (discussing State Department resistance).

136 Henry Farrell, *Trump's Plan to Work with Putin on Cybersecurity Makes No Sense. Here's Why.,* WASHINGTON POST (July 9, 2017), https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/09/trumps-plan-to-work-with-putin-on-cybersecurity-makes-no-sense-heres-why/?utm_term=.588bdb163087.

137 *Id.*

138 Karl de Vries, *Trump Appears to Back Away from Cybersecurity Effort with Putin*, CNN (July 10, 2017), http://edition.cnn.com/2017/07/09/politics/donald-trump-vladimir-putin-cybersecurity/index.html.

139 Schmitt *supra* note 63, at 177.

140 *Id.*

141 *Id*. at 177–178.

of nuclear weapons[142] supports Schmitt's statement. The nine nation-states holding nuclear weapons refused to attend negotiations.[143] Nevertheless, the U.N. agreed to the text and adopted the treaty.

We should not downplay the importance of this. It is only once first principles are put in place that progress can follow. Although it might take some time, the world is now inarguably at least one-step closer towards the total elimination of nuclear warfare. On the other hand, and as a counter to Schmitt's argument, there is precedent in international law for nation-states limiting their own freedom of action in certain areas, in spite of their perceived strength in those domains.[144] For example, 98% of the world's countries are party to the Chemical Weapons Convention, including those with the strongest capabilities to create and use such weapons.[145] This lends support to the idea that where certain acts are considered so grave, they can be internationally accepted as intolerable, regardless of nation strength or capability in that field. Why can that principle not be applied to cyberwarfare, albeit it in a more limited scope?

The value of international cooperation should not be understated. The only way for states to limit destabilizing activities in cyberspace and to prevent cyberattacks is to put these limits in place themselves. In fact, I would argue that global governments have an overt responsibility to do so, in order to protect their citizens. One of any state's key prerogatives should be to protect its own people from harm. This responsibility derives from the state's basic social contract or fiduciary relationship with its people.[146]

It is in every state's common interest to come to a binding agreement on cyber use of force by nation-states. We need to preempt a large-scale cyberattack that causes damage to another state's critical infrastructure and injury to civilians, if only

---

142 U.N. GAOR, *Draft Treaty on the Prohibition of Nuclear Weapons*, U.N. Doc. A/CONF.229/2017/L.3/Rev.1 (July 6, 2017).

143 Jen Maman, *Historic Day at the U.N.: Nuclear Weapons Are Now Banned Under International Law*, GREENPEACE (July 10, 2017), https://www.greenpeace.org.au/blog/historic-day-un-nuclear-weapons-now-banned-international-law/.

144 *See* Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Sept. 3, 1992, 1974 U.N.T.S. 45 (indicating the various nations who have signed on to the Chemical Weapons Convention and limiting their own freedom).

145 *Id.*

146 William C. Banks & Evan J. Criddle, *Customary Constraints on the Use of Force: Article 51 with an American Accent,* 29 LEIDEN J. OF INT'L L. 67, 74 (2016).

because it is not a case of, "will an attack of this type occur?" but "when will this type of attack occur?" Surely, it would be preferable to have the requisite laws in place so that the extent of any damage caused could be controlled and so the offending state could be sanctioned, rather than waiting for the attack to occur and then using it as the impetus to draft the law.

However, before attempting to draft such a global convention or cyber charter, we need to recognize that every state has different policies and interests at stake. For example, the U.S. and China take vastly different approaches to censorship, privacy, and other social and political values.[147] For that reason, it will not be possible to subject all aspects of cyberspace to international agreement. Furthermore, and as noted by Abraham D. Sofaer, there are other elements that we may not want to reach international agreement on, such as sharing information on cyber vulnerabilities.[148] He states, "[s]haring and improving the defensive capacities of all states would result in strengthening those whose networks the U.S. itself may seek to penetrate for intelligence or other purposes."[149] However, I would not read this as a bar to reaching a binding international agreement. A solution to these challenges lies in carefully drafting and confining the treaty's scope.[150]

An international treaty will only be possible if it has due regard to the substantial differences in international policy and agendas. While these factors limit the potential scope of an international cyber treaty, they should not deter nation-states from agreeing to a more controlled form of treaty. Nor should the international community discount the potential utility of such a treaty.

> International agreements covering other transnational activities, including armed conflict, communications, air and sea transportation, and health, agriculture, and commerce, among other areas, have been widely adopted by states to enhance safety and efficiency through

---

147 *See, e.g.*, Yanfang Wu et al., *A Comparative Study of Online Privacy Regulations in the U.S. and China*, 35 TELECOMM. POL'Y 603, 613 (2011) (discussing the differences in online privacy regulations between the U.S. and China).

148 Abraham D. Sofaer et al., *Cyber Security and International Agreements*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 179, 190–91 (Nat'l Acads. Press ed., 2010).

149 *Id.* at 191.

150 *See* Goldsmith, *supra* note 79, at 12 (commenting on the potential ability of multilateral agreements to increase stability and decrease miscalculation risks and the possibility of a narrower treaty for cooperation among like-minded states).

> processes that could well be useful in regulating cyber activities.[151]

No doubt, disputes will arise in negotiations, and there will be a number of problems and teething issues, in particular in verifying and attributing attacks and in ensuring compliance. Those who argue against new international cyber laws point to these factors as insurmountable hurdles.[152] However, if difficulties in attribution and fears of non-compliance were of themselves valid reasons not to enact laws, we would never pass any legislation. By way of example, anti-pollution laws are notoriously difficult to prosecute, and many people do not comply with their terms, nor do they view pollution as a crime.[153] Does this mean that the law should turn a blind eye, or should never seek to deal with problems in this field by way of legislation? Of course not.

A potential solution is as follows: We could select uncontroversial, settled principles of international law, and apply them to limited areas of cyber operations. For example, take Article 2(4) of the U.N. Charter and draft similar language for an international U.N. Cyber Charter, effectively prohibiting one state from using an unprovoked act of cyber force to target another state's independence, civilians or critical infrastructure systems. Nothing in this treaty would limit the ability of a state to resort to cyber force in an act of self-defense, or limit state action where states are already engaged in cyberattacks against one another. The core aim of this U.N. Cyber Charter would be the protection of civilians and the infrastructure that they rely on. The success of this charter could be realized through a regime that:

> (1) Applies generally accepted principles of international law to cyberspace. A crucial first step would be setting down agreed definitions of "critical national infrastructure,"[154] "cyberattack," "cyber force," and what I

---

151 Sofaer et al., *supra* note 148, at 180.

152 *See* Goldsmith, *supra* note 79, at 6–7, 10 (examining the major hurdles associated with a global cybersecurity treaty, such as a lack of mutual interest, inadequate U.S. concessions for reciprocal benefits, and verification problems).

153 *See, e.g.*, Michael Watson, *The Enforcement of Environmental Law: Civil or Criminal Penalties?* 17 ENVTL. L. & MGMT. 3, 3, 5 (2005) (describing implications associated with the prosecution of individuals who have committed environ mental offenses).

154 *See* discussion *supra* Part I.A (basing this definition on those provided by the Department of Homeland Security and European Union, but expanding it to expressly include democratic processes and election systems, including voting machines and connected apparatuses).

would term "acute cyberattack."[155] Nation-states would then formally acknowledge in the charter that an unprovoked state cyberattack, or state-sponsored cyberattack, on critical national infrastructure or on civilian targets would be an act of cyber force. Where an act of cyber force is grave enough to amount to an acute cyberattack, a state may resort to recognized principles of self-defense.

(2) Makes clear that nothing in the charter limits a state's ability to attack military targets, or limits other forms of cyber activity such as cyber exploitation.[156]

(3) Makes clear that nothing in the charter will operate to oblige signatories to divulge state information or national security information with another member-state.

(4) Establishes an independent body that will be accountable for oversight of the area and for verifying and attributing cyberattacks. This body should comprise ICT experts from the governments and the private sectors of each member-state. The independent body will be responsible for investigating cyberattacks when they occur. Crucially, their findings should be publicly disclosed where they have evidence that connects cyberattacks to a nation-state(s). This public disclosure should incentivize good behavior by member-states.

(5) Provides for remedies, including economic sanctions, countermeasures, and/or compensation in the event that a breach of the charter occurs.

Admittedly, the above proposal is restricted in its scope. It is not a perfect instrument. In particular, it does not go far enough to limit cyber vandalism or cyber exploitation by states (topics that warrant greater legislative attention, but which are outside the

---

[155] *See* Schmitt, *supra* note 63, at 163 (defining in a way like our current understanding of a traditional armed attack—that death or injury of persons was caused, or that there was a significant risk of this, and/or damage to or destruction of property).

[156] *See* Jack Goldsmith, *How Cyber Changes the Laws of War*, 24 EUR. J. INT'L L. 129, 130 (2013) (distinguishing the two forms of cyber threats: cyber exploitation and cyberattack). "Cyber exploitations . . . involve no disruption, but refer to merely monitoring and related espionage on computer systems, as well as the copying of data that is on those systems. Examples include the theft of credit card information, trade secrets, health records or weapons software and the interception of vital business, military and intelligence communications." *Id.*

reach of this essay). Smith's proposal for a Digital Geneva Convention is more ambitious.[157] He would have the world's governments commit not to build or stockpile cyber weapons in any circumstance.[158] He also advocates for a global technology sector that would act as a neutral "Digital Switzerland," where no private technology industries would engage in cyberattacks and where large technology companies would assist the victims of cyberattacks.[159] While these are both admirable aims, I would argue that they should be eventual goals rather than primary targets. If the initial charter—or whatever form the global agreement is to take—overreaches, it will be very difficult to bring all the world's nations to the table. As a matter of priority, we should first endeavor to put a global charter in place agreeing not to attack one another's critical national infrastructure in times of peace using cyberattacks. Once we agree on that initial principle, which is a lofty goal in and of itself, then we can enhance and build on that agreement. The U.N. Cyber Charter is not the final solution; it is the starting point.

Importantly, nation-states should be careful not to view any international treaty or charter as a panacea. Countries around the world should continue to take national steps and develop independent and defensive strategies to prevent attacks and increase their own intelligence.

VI. CONCLUSION

Over the last number of years, the international community has sat back and watched as the number of cyberattacks has accelerated. In recent months, we have seen nation-states mount attacks on critical national infrastructure, including electricity grids and democratic voting systems. Civilians have been left in the dark and unable to communicate with one another. Arguments have been raised that Americans were denied their right to elect their own leader. The fact that there is even a seed of doubt about that is chilling. Cyberattacks have entered a new and dangerous

---

157 *See* Smith, *supra* note 128 (recognizing a need for the world's governments to come together as an industry to protect civilians on the Internet, analogous to the 1949 Geneva Convention, which sought to protect civilians in times of war).

158 *See id.* (discussing the need for the world's governments "to pledge that they will not engage in cyberattacks on the private sector" and will instead "work with the private sector to respond to vulnerabilities").

159 *See id.* (advocating a need for a global industry that only plays defense in the realm of cyberattacks).

era. An acute cyberattack that could threaten global stability is potentially just around the corner. Anticipating and planning for the worst should drive our next steps. Our international law must focus more on preventative measures instead of reacting after an attack occurs. In fact, to adopt any other approach at this point would be negligent. We know that these attacks are coming. We should call on our governments to protect us and to protect the systems that we hold dear, such as democracy and technological innovation. We need to come together and work in earnest to find a solution and to reach an agreement as to how states may behave in cyberspace. This will ensure that we can safely utilize all that the Internet has to offer and live in an increasingly interconnected and ICT-fueled world without fear.