

Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community

Colonel David Wallace &
Lt. Colonel Mark Visger*

“They came together in 1949 in Geneva Switzerland and that is what led to the recognition that they needed the fourth Geneva Convention to protect civilians in times of war. Now it the time for us to call on governments to protect civilians on the internet in times of peace.”

Brad Smith, President of Microsoft Incorporated

* Colonel David Wallace is Professor and Head of the Department of Law at the U.S. Military Academy, West Point, New York. Lieutenant Colonel Mark Visger is a Judge Advocate in the U.S. Army and an Assistant Professor in the Department of Law at the U.S. Military Academy. Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia in 2017. Colonel Wallace would like to thank the NATO CCD COE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship. The authors would like to thank Lieutenant Colonel Shane Reeves and Professor Robert Barnsby for their support and assistance. The views expressed herein are personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, any other department or agency of the United States Government or the NATO CCD COE. The analysis presented herein stems from academic research of publicly available sources, not protected operational information.

ABSTRACT

In February 2017, Brad Smith, President of Microsoft, electrified the technology community with a speech to the RSA Conference calling for a “Digital Geneva Convention” to stem the flow of State cyber operations that have become endemic. Despite good intentions, Smith’s call for a Digital Geneva Convention is based, in part, on a misunderstanding of the state of international law as it applies to cyber. In fact, there already exists a robustly developed set of international law norms, although enforcement of these norms remains problematic. In addition, Smith’s call for a Digital Geneva Convention overlooks the need for States to agree to adopt such a treaty. Despite these limitations, tech sector involvement in the international law process has the potential to develop the law in a positive direction and should be encouraged. However, such tech sector involvement requires an appreciation for international law and the current state of the law as it applies to cyber operations. With this foundation, the tech sector will be able to properly engage in the international law process to develop the law applicable to cyber operations to address their concerns.

INTRODUCTION & BACKGROUND

At the RSA Conference in San Francisco on February 14, 2017, Brad Smith, the President of Microsoft Corporation, gave a keynote address entitled “Protecting and Defending against Cyberthreats in Uncertain Times.”¹ Smith

¹ Brad Smith, Protecting and Defending against Cyberthreats in Uncertain Times, RSA Conference, <https://www.rsaconference.com/videos/protecting-and-defending->

highlighted, among other things, the troubling fact that in recent years there has been an expansion of incidents of States engaging in cyber operations against other States.² Smith contended that the 2014 Sony cyber-attack by North Korea was a turning point.³ In that operation, a group calling themselves “Guardians of Peace” hacked into Sony Pictures. The United States has alleged that the Guardians of Peace were a cyber proxy for North Korea.⁴ The hackers stole confidential documents and data from the Hollywood studio and posted them online and deleted other files.⁵ It is believed by U.S. government officials that North Korea used the Guardians of Peace to target Sony because it backed the film, “The Interview,” which depicts an assassination plot against the North Korean leader, Kim Jong-Un.⁶ Commenting on the incident, Smith noted that the Sony cyberattack was “not for espionage, not related to the military, but to attack a private company for engaging in freedom of expression around, as it turned out, not a terribly popular movie.”⁷

Using militaristic language and imagery, Smith

against-cyberthreats-in-uncertain-times (last visited Jan. 16, 2018).

² *Id.*

³ *Id.*

⁴ Ellen Nakashima, Craig Timberg & Andrea Peterson, *Sony Pictures hack appears to be linked to North Korea, investigators say*, Washington Post (Dec. 3, 2014), https://www.washingtonpost.com/world/national-security/hack-at-sony-pictures-appears-linked-to-north-korea/2014/12/03/6c3c7e3e-7b25-11e4-b821-503cc7efed9e_story.html?utm_term=.8d3e4029c075. Smith showed this webpage on his slides while discussing this attack.

⁵ *Id.*

⁶ Andrea Peterson, *The Sony Pictures hack, explained*, Washington Post (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b8aac1f6ebdc (last visited Aug. 7, 2017).

⁷ Smith, *supra* note 1.

described cyberspace as a new battlefield, albeit different than other war fighting domains of land, sea and air. Underscoring cyberspace's unique and different nature, Smith commented that cyberspace is owned and operated by the private sector whether "it's submarine cables or datacenters or servers or laptops or smartphones."⁸ He also posited that companies like Microsoft are the "world's first responders" to cyberattacks by States.⁹ After framing the problem of increased State cyber-attacks, Smith offered, for consideration, three responses to such actions. First, he argued for greater vigilance in that companies and individuals need to do more (and more together) in terms of cyber security even though there are many new and important things already being done.¹⁰ Second, Smith laid out arguments for a new international treaty.¹¹ He specifically noted that "[The world's governments] came together in 1949 in Geneva Switzerland and that is what led to the recognition that they needed the fourth Geneva Convention to protect civilians in times of war. Now it the time for us to call on governments to protect civilians on the internet in times of peace."¹² In calling for a new "Digital

⁸ Smith, *supra* note 1. In making this comment, Smith seemed to marginalized or discount responses to State cyber-attacks by the government of the victim State. He specifically stated that [i]nstead of nation-state attacks being met by responses from other nation-states, they are being met by us."

⁹ *Id.*

¹⁰ *Id.* With regard to this point, Smith was not only advocating better computer hygiene, individually and collectively, but also new computer security tools and better organizational structures and response capabilities.

¹¹ *Id.*

¹² *Id.* The entire list of proposals for the Digital Geneva Convention can be found at 11:43 of the video. They include: "1. No targeting of tech companies, private sector or critical infrastructure; 2. Assist

Geneva Convention,” he pointed out that there have already been international cooperative efforts, both bi-laterally and multi-laterally, to establish new sets of norms.¹³ In the context of the Digital Geneva Convention, he also advocated for the establishment of an independent organization, like the International Atomic Energy Agency¹⁴ which has addressed issues related to nuclear proliferation, to bring together the best and brightest from the private and public sectors as well as academia.¹⁵ The purpose of this new international organization would be to not only observe what is happening in cyberspace between and among States, but also to identify attackers.¹⁶

Smith’s third idea is that the global technology sector must become a trusted and neutral “Digital Switzerland” on which everyone can rely. This proposal is rooted, in part, in the significant role the International Committee of the Red Cross (ICRC) plays in the protection of the victims of armed conflict.¹⁷ More specifically, the ICRC is an independent, neutral organization that ensures humanitarian protection and assistance for victims of armed conflict and other

private sector efforts to detect, contain, respond to and recover from events; 3. Report vulnerabilities to vendors rather than to stockpile, sell or exploit them; 4. Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise and not reusable; 5. Commit to nonproliferation activities to cyber weapons; 6. Limit offensive operations to avoid a mass event.

¹³ *Id.*

¹⁴ See International Atomic Energy Agency (IAEA), *Official Web Site of the IAEA International Atomic Energy Agency (IAEA)*, <https://www.iaea.org/> (last visited Aug 8, 2017).

¹⁵ Smith, *supra* note 1.

¹⁶ *Id.*

¹⁷ See International Committee of the Red Cross, *International Committee of the Red Cross*, <https://www.icrc.org/en> (last visited Aug 8, 2017).

situations of violence.¹⁸ It also promotes respect for the law of armed conflict and its implementation in national law.¹⁹ In his speech, Smith draws parallels between the potential role and contributions of the global technology sector and the ICRC in terms of dealing with cyber security threats from States.

Smith is absolutely correct that there is an increasing threat of State cyber-attacks. In some cases, the cyberattacks happened in the context of an armed conflict while at other times the operations occurred during peacetime. For example, there was a Russian cyber campaign against Georgia immediately before and during their 2008 armed conflict whereby so-called Russian patriot hackers targeted Georgian government and news websites with Distributed Denial of Service (DDoS) attacks.²⁰ In 2010, the so-called Stuxnet worm was reportedly launched against Iranian uranium-enrichment centrifuges causing some of them to speed up thereby destroying them.²¹ More recently, there were the so-called WannaCry and Petya ransomware attacks which crippled hundreds of thousands of computers worldwide with the perpetrators of the attacks demanding digital ransom from the machines owners to regain access.²² Last, but certainly not least, is the alleged Russian cyber

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ SHAKARIAN, PAULO, JANA SHAKARIAN, ANDREW RUEF & SUSHIL JAJODIA, INTRODUCTION TO CYBER-WARFARE A MULTIDISCIPLINARY APPROACH, 24 (2013).

²¹ BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES: CONFRONTING A NEW AGE OF THREAT 23 (2017).

²² Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, The New York Times (June 27, 2017), <https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html> (last visited Aug 7, 2017).

operation against the U.S. electoral system.²³

Smith is not the only one that has called for a Digital Geneva Convention.²⁴ But given that he is the President of Microsoft Corporation; that there has been a spate of recent cyber operations by State actors or their proxies; and that increasingly more States are developing sophisticated cyber conflict capabilities, Smith's remarks exploded across the Internet. Moreover, the visceral appeal for such a cyber-specific treaty is greatly enhanced when linked to the 1949 Geneva Conventions, which are the most or one of the most well-known and highly regarded treaties in the history of humankind.²⁵

This article will focus on Smith's proposal for a Digital Geneva Convention and, to a lesser extent, on his ideas for the establishment of an international, independent watchdog agency like the International Atomic Energy Agency and for the global technology sector becoming a trusted and neutral Digital Switzerland. Smith's speech should be viewed as an important step towards the improved rule of law in cyber operations, and a step that one hopes will continue to fruition. Smith's proposal, however, was made to a forum of technology experts and not to the international and legal community which is currently working on these issues. As such, it overlooks the significant work that has

²³ Michael Riley & Jordan Robertson, *Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known*, Bloomberg (June 13, 2017), <https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections>.

²⁴ Rachael Kalinyak, *Companies want a Digital Geneva Convention; researchers demur*, Defense News (July 18, 2017), <http://www.defensenews.com/home/2017/07/18/companies-fighting-for-a-digital-geneva-convention-for-cybercrime/>.

²⁵ GARY D. SOLIS, *THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR* 88 (2d ed. 2016).

already been accomplished in this area, such as the drafting and publication of the 2017 *Tallinn Manual 2.0*, which is a restatement of the international law as it currently exists with respect to cyber by a group of international experts.²⁶ In addition, Smith's proposal frames certain issues and uses analogies in ways that do not match the legal framework developed to date. As an example, Smith calls for a Digital Geneva Convention, which is understandable given the ubiquity and broad acceptance of this treaty. However, in practice, his specific proposals track more closely with the prohibitions on the use of force found in the U.N. Charter. In addition, his proposal overlooks the key dynamics by which international law is created, particularly through the adoption of treaties and customary law--both of which require significant State buy-in due to the need for State consent to such legal provisions. As a result, Smith and the technology community will need to persuade States to view his proposals as being in their best interest.

This article is written to encourage greater dialogue between the technology community and the international law community to achieve common terms of reference and a common understanding of the legal and technological challenges posed by cyberspace and operations. The technology community as a whole, and Smith's proposals in particular, offer insights and potential methods by which the legal norms could be developed. The international law community has been working on challenges posed by cyber for some time and provides a significant foundation to build upon to reach consensus on the international law framework for cyber operations. This article will review the

²⁶ TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt ed., 2d ed 2017) [hereinafter TALLINN MANUAL 2.0].

international law framework currently governing cyber and analyze how it would apply to the attacks cited by Smith. It will next turn to the need for State buy-in and consent to the multi-lateral treaty framework proposed by Smith, which is currently not likely. Finally, the article will review how the technology sector could assist in the development of a more effective international law framework governing cyber operations.

I. SMITH'S PROPOSAL IMPLIES A NORMATIVE VOID IN INTERNATIONAL LAW

A. *The Foundational Structure of International Law*

For the technology community to appreciate the process by which a Digital Geneva Convention would be formed, it must understand the dynamics of the international legal system. Generally speaking, public international law is a body of law which is legally binding on States in their sovereign capacity (and not private individuals) in their intercourse with each other.²⁷ However, one cannot appeal to the UN General Assembly or similar world super-legislature to enact Smith's proposal of a Digital Geneva Convention as binding international law. Instead, there are

²⁷ ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICT 5 (2010). It is important to note that States are not the only subjects of international law. Individuals and international organizations may also fall under the purview of international law. Additionally, public international law is distinguished from private international law in that the latter is the rules that are established or agreed upon by citizens of different nations who privately enter into transactions and that will govern in the event of a conflict.

other, slightly different legal sources to consider. The Statute of the International Court of Justice recognizes three primary sources of international law:

- (a) “international conventions” [*e.g.*, treaties]
- (b) “international custom, as evidence of a general practice accepted as law”
- (c) “the general principles of law recognized by civilized nations”²⁸

These sources reveal an important element of international law—consent. States generally must consent to a legal obligation before they are obligated to abide by it. Such was stated in the classic international law case, *S.S. Lotus*,²⁹ but it can be seen in the two primary sources of international law: treaties and custom. Treaties by their nature require states to explicitly consent to be bound by the treaty requirements.³⁰ Custom does the same, albeit indirectly—the international law of custom allows states to

²⁸ Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1055 [hereinafter *Statute of the ICJ*]. The Statute also cites, as a “subsidiary means” to determine the law, “judicial decisions and the teaching of the most highly qualified publicists [scholars] of the various nations.”

²⁹ *S.S. Lotus* (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 at para. 144 (Sept. 7). In this case, the Court famously noted: “International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.” *Id.*

³⁰ See Vienna Convention on the Law of Treaties, arts. 11-16, May 23, 1969, 1155 U.N.T.S. 331 (specifying the means of a state to express its consent to be bound by a treaty).

be a “persistent objector” as binding customary law is formed.³¹ As a result, when it comes to customary law, silence to a developing customary legal norm can be considered to be *de facto* consent. Viewed through the prism of law-making, public international law generally is a relatively primitive legal system.³² There are no legal institutions that are comparable to national legislatures with the power to promulgate laws of general applicability and no executive to enforce existing laws, instead States must enforce international law amongst themselves as sovereign equals, unless enforcement power has been delegated to a supra-national governance and judicial bodies such as the European Union or International Criminal Court. As a result, public international law is not created, interpreted, and enforced though the kinds of institutions found in domestic legal systems. Accordingly, as a body of law, it has had to justify its legitimacy and reality over the centuries.³³ At the extreme, there are even some highly respected commentators who take and argue the position that international law is not law at all. Rather, it is a special kind of politics where States coordinate their efforts to maximize their interests.³⁴ This view of public international law is neither new nor novel.

Another critical aspect of the international law process is that it is self-enforcing. That is, States enforce

³¹ INT’L LAW ASS’N, STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW, principle 15 (2000) [hereinafter ILA CUSTOMARY LAW PRINCIPLES].

³² THOMAS BUERGENTHAL & HAROLD G. MAIER, PUBLIC INTERNATIONAL LAW IN A NUTSHELL 19 (1985).

³³ LORI FISLER DAMROSCH & SEAN D. MURPHY, INTERNATIONAL LAW: CASES AND MATERIALS 1 (6th ed. 2009).

³⁴ MARY ELLEN O’CONNELL, THE POWER AND PURPOSE OF INTERNATIONAL LAW: INSIGHTS FROM THE THEORY AND PRACTICE OF ENFORCEMENT 2 (2011).

international law amongst themselves as sovereign equals.³⁵ This is most commonly seen through the doctrines of countermeasures and retorsion. Countermeasures are measures taken by States that themselves violate international law but are justified because they are done in response to a violation of international law by the targeted State.³⁶ Retorsion is similar—they are unfriendly measures that do not violate international law taken to show disapproval of the target's violation of international law.³⁷ President Obama's expulsion of Russian diplomats in response to alleged Russian cyber operations during the 2016 election has been reasonably characterized as retorsion.³⁸ Additional enforcement measures, such as enforcement actions by an independent enforcement body, can only exist if States agree to them, much like if they must consent to a treaty obligation. Examples of enforcement bodies include, but are not limited to, the UN Security Council, which is authorized to take action in response to threats to international peace and security³⁹ or the International Criminal Court, in which States have agreed to jurisdiction for war crimes under certain circumstances.⁴⁰

Although international law is often maligned or

³⁵ FISLER & MURPHY, *supra* note 33, at 1.

³⁶ Int'l Law Comm'm, Responsibility of States for Internationally Wrongful Acts, art. 22, GA Res. 56/83 annex, UN Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter, Articles on State Responsibility]. Much like the Tallinn Manual 2.0, these articles represent a restatement of customary international law by the International Law Commission.

³⁷ *Id.*, *chapeau* to Chapter II of Part 3, para. 3.

³⁸ Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 Har. Nat. Sec. J. 239, 258 (2017).

³⁹ UN Charter, art 39.

⁴⁰ Rome Statute of the International Criminal Court, art. 1, July 17, 1998, 2187 U.N.T.S. 90.

marginalized and most certainly has shortcomings, it is widely accepted that “almost all nations observe almost all principles of international law and almost all of their obligations almost all of the time.”⁴¹ Speaking on the value and importance of international law, law professor Mary Ellen O’Connell observed:

International law has deficits, yet it persists as the single, generally accepted means to solve the world’s problems. It is not religion or ideology that the world has in common, but international law. Through international law, diverse cultures can reach consensus about the moral normal that we will commonly live by. As a result, international law is uniquely situated to mitigate the problems of armed conflict, terrorism, human rights abuse, poverty, disease, and the destruction of the natural environment. It is the closest thing we have to a neutral vehicle for taking on the world’s most complex issues and pressing problems.⁴²

In short, international law is a constantly evolving set of legal norms that are commonly observed by States in their relations with one another that confer rights and impose obligations in both peace and wartime.⁴³

⁴¹ LOUIS HENKIN, *HOW NATIONS BEHAVE: LAW AND FOREIGN POLICY* 47 (1979).

⁴² O’CONNELL, *supra* note 34, at 14.

⁴³ EDWARD COLLINS, JR., *INTERNATIONAL LAW IN A CHANGING WORLD: CASES, DOCUMENTS, AND READINGS* 2 (1970).

B. Current Regimes Affecting Cyber: Governing Treaty and Customary Law

This section will examine the current international law provisions affecting cyber. Throughout Smith's talk, he implied that a normative legal void exists regarding cyber-attacks conducted by States. As will be seen below, this is not the case. In fact, there is extensive international law that applies and, in fact, many of the cyber-attacks that Smith cites are prohibited under international law. This section will outline the legal framework and then apply it to the cyber-attacks noted in Smith's talk. Ultimately, what will be seen is that the inherent weakness of the international law enforcement framework combined with the problem of attribution limits strong enforcement of the current existing law, resulting in a perception of a normative legal void in this area. As noted above, much of international law is comprised of customary law and there have been several attempts to restate current customary law as it applies to cyber, which shed helpful light on the current state of the law.⁴⁴

⁴⁴ In the arena of customary law, it is common for academic and government experts to distill current state practice into statements of governing customary law. As noted by the Supreme Court, "where there is no treaty and no controlling executive or legislative act or judicial decision, resort must be had to the customs and usages of civilized nations, and, as evidence of these, to the works of jurists and commentators who by years of labor, research, and experience have made themselves peculiarly well acquainted with the subjects of which they treat. Such works are resorted to by judicial tribunals, not for the speculations of their authors concerning what the law ought to be, but for trustworthy evidence of what the law really is." *The Paquete Habana*, 175 U.S. 677, 700 (1900).

1. Tallinn Manual/GGE Processes

The previous explanation of the international law development process provides a foundation for the work of experts to distill the international legal provisions currently in effect and apply them to the challenges posed by cyberspace and operations. This process is not unusual to the law, as lawyers frequently use existing legal frameworks and doctrines and extend them, by analogy, to novel subject areas such as the international regulation of emerging technologies. While a debate exists as to feasibility of extending current legal doctrine to cyberspace and operations, this is the starting point, at a minimum.

With respect to the Tallinn process, in 2009, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), a renowned cyber research and training institution in Tallinn, Estonia, invited a group of experts to produce a manual on the international law governing cyber warfare.⁴⁵ This project brought together a distinguished group of international law scholars and practitioners to explore and articulate how extant legal norms apply to cyber warfare.⁴⁶ Namely, the experts examined both treaty provisions that may be extended to cyberspace and operations and whether current state practice has solidified to the point that it may be considered customary international law. Although much of international law is thought of as treaty law, customary law still plays an important role in developing and binding States.⁴⁷ Customary international law is defined as a general practice

⁴⁵ TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael Schmitt ed. 2013) [hereinafter TALLINN MANUAL].

⁴⁶ *Id.*

⁴⁷ A.P.V. ROGERS, LAW ON THE BATTLEFIELD 2 (2004).

of law under Article 38(1)(b) of the Statute of the International Court of Justice, which States follow out of a sense of legal obligation.⁴⁸ Put in a slightly different manner, customary international law results from the general and consistent practice of States that is followed by them from a sense of legal obligation.⁴⁹ Customary international law is binding on all States except in those circumstances in which a state consistently and unequivocally refused to accept a customary practice.⁵⁰

In 2013, the *Tallinn Manual on International Law Applicable to Cyber Warfare* was published and released.⁵¹ As a result of the success of this first Tallinn Manual, the NATO CCD COE initiated a follow-on project to expand the scope of coverage with an updated manual to include the international law governing cyber activities during peacetime as well as wartime. The NATO CCD COE convened a second group of international experts for the follow-on effort.⁵² Their dedicated work led to the creation and publication of *Tallinn Manual 2.0* in 2017.⁵³ The significantly expanded Manual not only incorporated and updated the materials from the first Tallinn Manual, but also included coverage of legal regimes implicated by peacetime cyber activities and incidents.⁵⁴ Impressively, *Tallinn Manual 2.0* has 154 unanimously agreed upon rules with

⁴⁸ *Statute of the ICJ*, *supra* note 28.

⁴⁹ Theodor Meron, *Customary Law*, in *CRIMES OF WAR 2.0 WHAT THE PUBLIC SHOULD KNOW*, 141 (Roy Gutman, David Rieff, & Anthony Dworkin, eds., 2007).

⁵⁰ ADAM ROBERTS & RICHARD GUELFF, *DOCUMENTS ON THE LAWS OF WAR* 7 (3rd ed. 2000).

⁵¹ *TALLINN MANUAL*, *supra* note 45.

⁵² *TALLINN MANUAL 2.0*, *supra* note 26, at 1.

⁵³ *Id.*

⁵⁴ *Id.*

detailed commentary accompanying each rule which not only offers some tremendously important insights into the deliberations and thought processes of the experts regarding the legal basis and justification for the rules and their normative context, but also offers practical implications of the rules' application in a cyber context. This level of detail is particularly helpful for national legal advisors and academics. Additionally, the commentaries to the rules articulate positions by the experts in their discussions such that it is makes clear when either the experts all reached agreement or when they could not reach consensus on a specific issue.

Despite the great helpfulness of *Tallinn Manual 2.0*, its limitations must also be noted. It is important to reiterate that the experts were limiting themselves to a restatement of the *lex lata*, i.e., the law as it exists, and avoided including statements reflecting the *lex ferenda*, i.e., what the law should be.⁵⁵ Given the ephemeral process of determining customary law, the Tallinn process was not an unusual activity for international law experts, as they will frequently summarize current state practice and *opinio juris* to determine the law as it really is.⁵⁶ In addition, the *Tallinn Manual 2.0* clearly indicates that this effort was intended to be an expression of the opinions of the experts as to the current state of the law and is not an official document.⁵⁷ Despite this fact, the robust framework of the 154 rules unanimously agreed to by the international group of experts is strong evidence of the evolution of customary law that has taken place to address cyber operations. As a result, it can hardly be said that there is a legal normative void regarding

⁵⁵ *Id* at 3.

⁵⁶ *The Paquete Habana*, 175 U.S. at 700.

⁵⁷ TALLINN MANUAL 2.0, *supra* note 45, at 2.

cyberspace and operations. In fact, as will be detailed later, each of the cyber operations Mr. Smith cited in his speech are addressed in the legal framework articulated in *Tallinn Manual 2.0*.

An important part of the process of creating *Tallinn Manual 2.0* was the so-called “Hague Process” hosted by the Netherlands Ministry of Foreign Affairs.⁵⁸ The Dutch convened States to unofficially comment on working drafts of *Tallinn Manual 2.0*.⁵⁹ Over 50 States and international organizations participated in the process in a Chatham House environment in three two day sessions.⁶⁰ Additionally, some States provided unofficial written feedback on the working drafts of *Tallinn Manual 2.0*, which led to a refinement of the text.⁶¹ There was no such Hague process used with the first Tallinn Manual. Such collaborative interest and input for *Tallinn Manual 2.0* highlights how well regarded and received the Tallinn Manuals and process are for the international community. In addition to the Hague Process, the United Nations also attempted to facilitate discussions on cyberspace and operations between and among States. They did this through the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (otherwise known as the Group of Governmental Experts, or GGE).⁶²

The GGE is a UN-mandated working group

⁵⁸ *Id.* at 6.

⁵⁹ *Id.*

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, Just Security (June 30, 2017), <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>.

consisting of representatives from interested States focused on information security. The GGE process was established to create ongoing dialogue and consensus among States regarding the implications of the new technologies and the building of an international framework to promote security and stability with respect to information technology.⁶³ Until mid-2017, the GGE had achieved modest success, issuing two reports outlining principles on which there was consensus—an important starting point for the development of customary law.⁶⁴ Progress on this front has since stalled due to a breakdown in consensus.⁶⁵ Prior to this point there had been some progress, progress which was even noted by Smith in his RSA talk.⁶⁶ Notwithstanding the obvious disappointment at the GGE's failure to advance international cyber norms through inter-State discussions in 2017, it is encouraging that some progress has been made over the past five years through the promotion and development of cyber customary law like the Tallinn Manuals, the Hague process, and two earlier GGE reports. As will be discussed in greater detail below, the collapse of the GGE process speaks volumes about the difficulties of attaining the broad

⁶³ G.A. Res. 66/24, para. 4, A/RES/66/24 (Dec. 2, 2011).

⁶⁴ U.N. Group of Governmental Experts, Rep., transmitted by letter dated June 26, 2015, by the Chair of the group established pursuant to G.A. Res. 66/24 (2011), concerning Developments in the Field of Information and Telecommunications in the Context of International Security, para. 13, U.N. Doc A/70/174 (July 25, 2015)[hereinafter GGE 2015 report]; U.N. Group of Governmental Experts, Rep., transmitted by letter dated June 7, 2013, by the Chair of the group established pursuant to G.A. Res. 66/24 (2011), concerning Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 19-25, U.N. Doc A/68/98 (June 24, 2013)[hereinafter GGE 2013 report].

⁶⁵ Schmitt & Vihul, *supra* note 62.

⁶⁶ Smith, *supra* note 1.

agreement necessary to establish a multilateral treaty like a Digital Geneva Convention and how some States would prefer confusion over legal norms in cyberspace operations to preserve their relative freedom of action in the digital domain.⁶⁷

With this context, we can now turn to how current treaty and customary law applies to cyber operations. The most clear application is found in the Law of Armed Conflict. As noted in the *Tallinn Manual 2.0*, “[a]s with other operations, the law of armed conflict applies to cyber operations undertaken in the content of an armed conflict. Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the experts were unanimous in finding that the law of armed conflict applies to such activities during both international and non-international armed conflicts.”⁶⁸ This conclusion is significant because the 1949 Geneva Conventions, which will be discussed in detail below, are the single most important treaties comprising the law of armed conflict and is the centerpiece of Mr. Smith’s proposal. This assessment that existing international law applies to cyberspace operations has been acknowledged by NATO, two GGE reports in 2013 and 2015 and by most States.⁶⁹ Additionally, the International Court of Justice confirmed in its *Nuclear Weapons Advisory opinion* that the UN Charter’s Article 2(4) prohibition on the use of force and Article 51’s recognition of an inherent right of self-defense

⁶⁷ Robert McLaughlin & Michael Schmitt, *The need for clarity in international cyber law*, Policy Forum (Sept. 18, 2017), <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/>.

⁶⁸ TALLINN MANUAL 2.0, *supra* note 45, r.80, para.1.

⁶⁹ *Id.*

apply regardless of the weapon used.⁷⁰

2. *Jus in Bello*: Law of Armed Conflict

The four Geneva Conventions of 1949 are at the foundation of the law of armed conflict.⁷¹ The Geneva Conventions of 1949 are the most well-known and important treaties comprising the law of armed conflict. They are the most ratified international agreements in history.⁷² All of the

⁷⁰ Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 39 (July 8) [hereinafter Nuclear Weapons Opinion].

⁷¹ SOLIS, *supra* note 25, at 88.

⁷² *Id.* The origin of the Geneva Conventions and the birth of the International Committee of the Red Cross can be traced back to 19th Century warfare and the efforts of a young Swiss businessman, Henri Dunant. Traveling on business in northern Italy, Dunant witnessed the battle of Solferino and its aftermath. The battle of Solferino was fought alongside the Mincio River in the Lombardy region of the country. This June 1859 battle of approximately 300,000 men involved the French, allied to the Sardinians facing, the Austrian troops. In its wake, 6,000 men were killed and 40,000 were wounded. Dunant was horrified by the carnage and the sight of abandoned and untended wounded which was the military practice at the time. Along with local residents and other volunteers, Dunant cared for the wounded and dying for three days and nights. Dunant was so moved by this experienced, he self-published a small book, *A Memory of Solferino*. The book not only graphically depicted the brutality and unspeakable misery of warfare at that time, but also called for a plan of action – a proposal. Dunant advocated the formation of relief societies to care for wartime wounded – the future International Committee of the Red Cross. Additionally, he called for the adoption of an intentional convention which ultimately resulted in the adoption of the first Geneva Convention in 1864. This convention provided principles that called for relief to wounded without distinction as to nationality; neutrality of medical personnel and establishments and units; and the distinctive sign or protective emblem of the red cross on white background. International Committee of the Red Cross, *From the*

nations of the world have ratified the conventions.⁷³ Given their universal acceptance, it is not at all surprising that Smith used the conventions as a benchmark for the regulation of cyber armed conflict. Fundamentally, the Geneva Conventions of 1949 are aimed at limiting the barbarity of armed conflict and protecting the following categories of war victims respectively: wounded and sick on land, the wounded, sick, and shipwrecked at sea, prisoners of war and civilians. There were a number of important innovations represented in the Geneva Conventions of 1949. First, there was, for the first time, a requirement that States enact domestic legislation to prosecute those who committed grave breaches of the Conventions.⁷⁴ Second, ratifying States were obligated to search out and try individuals who committed grave breaches.⁷⁵ Third, and a related point to the initial two innovations, the category of grave breach was included in the Conventions.⁷⁶ Finally, Common Article 3 was incorporated in all four conventions thereby providing baseline humanitarian protections in non-international

battle of Solferino to the eve of the First World War, (Dec. 28, 2004), <https://www.icrc.org/eng/resources/documents/misc/57jnv.htm>.

⁷³ SOLIS, *supra* note 25, at 88.

⁷⁴ Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 49, Aug. 12, 1949, 75 U.N.T.S. 31 [hereinafter GCI]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 50, Aug. 12, 1949, 75 U.N.T.S. 85 [hereinafter GCII]; Geneva Convention relative to the Treatment of Prisoners of War art. 129, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter GCIII]; Geneva Convention relative to the Protection of Civilian Persons in Time of War art. 146, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter GCIV].

⁷⁵ *Id.*

⁷⁶ GCI, *supra* note 74, art. 50; GCII, *supra* note 74, art. 51; GCIII, *supra* note 74, art. 130; GCIV, *supra* note 74, art. 147.

armed conflicts.⁷⁷ After the adoption of the Geneva Conventions in of 1949, they were supplemented by two Additional Protocols in 1977 to address developments in the conduct of warfare, specifically addressing guerrilla-type internal armed conflicts and revolutionary movements that had become the norm.⁷⁸

The *Tallinn Manual 2.0*'s experts were unanimous in their opinion that the law of armed conflict (primarily codified in the Geneva Conventions and the Additional Protocols) applied to "cyber operations executed in the context of an armed conflict."⁷⁹ Their opinion was based in part on the statement of the International Court of Justice in the *Nuclear Weapons* advisory opinion, indicated that the law of armed conflict applies "to all forms of warfare, and to all kinds of weapons, those of the past, those of the present, and those of the future."⁸⁰ The *Tallinn Manual 2.0* ultimately specified 70 rules drawn from the law of armed conflict which govern cyber operations taking place during armed conflict.⁸¹ While one of the areas of disagreement leading to the breakdown of the 2017 GGE was whether the law of armed conflict applied,⁸² one would be hard pressed to say that the law of armed conflict does not apply to cyber operations in armed conflict.

⁷⁷ SOLIS, *supra* note 25, at 87-118.

⁷⁸ GARY D. SOLIS & FREDERIC L. BORCH, GENEVA CONVENTIONS 33 (2010).

⁷⁹ TALLINN MANUAL 2.0, *supra* note 26, r. 80 & para. 1.

⁸⁰ *Id.* at 451, para. 1, citing *Nuclear Weapons Opinion*, *supra* note 70, para. 86.

⁸¹ *Id.*, r. 80-149.

⁸² See notes 150-158, *infra*, and accompanying text.

3. Jus ad Bellum

To a lesser degree and more indirectly, Smith's proposals implicate a second body of international law that regulates the international use of force – *jus ad bellum*.⁸³ Both *jus in bello* (discussed above) and *jus ad bellum* involve the regulation of the use of force, but in separate and distinct ways. That is, the laws comprising a State's right to wage war and the rights and obligations that are triggered once war has started unequivocally operate as distinct normative universes.⁸⁴ Accordingly, *jus ad bellum* means the right to resort to force or right to wage war.⁸⁵ It defines the legitimate reasons a State may resort to an armed conflict.⁸⁶ The primary modern legal authority underpinning modern *jus ad bellum* is the United Nations Charter, which addresses the concept in two key provisions. The first is Article 2(4) which provides that "[a]ll members shall refrain in their international relations from threat or the use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purpose of the United Nations."⁸⁷ By prohibiting the use of force,

⁸³ C. Stahn, *Jus ad bellum, jus in bello . . . jus post bellum? -Rethinking the Conception of the Law of Armed Force*, 17 Eur. J. of Int'l Law 921, 922 (2006). Some commentators believe that this traditional dualist conception of the laws of war should be extended to a third period following hostilities namely *jus post bellum*. This third period would involve the regulation of the ending of conflicts and easing the transition to peace through certain the application of norm. *Id.*

⁸⁴ INGRID DETTER DE LUPIS FRANKOPAN, *THE LAW OF WAR* 156 (2000).

⁸⁵ KOLB & HYDE, *supra* Note 27, at 9.

⁸⁶ *What are jus ad bellum and jus in bello?*, INTERNAT'L COMMITTEE OF THE RED CROSS (Jan. 22, 2015), <https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0> (last visited Aug 15, 2017).

⁸⁷ UN Charter art. 2, para. 4.

rather than the somewhat anachronistic term war, the drafters of the Charter sought to avoid the debate about whether a particular conflict amounted to a war.⁸⁸ Leading scholars believe that the use of force between States is prohibited by a peremptory rule of international law.⁸⁹ The other provision is Article 51 of the United Nations Charter. It provides that “[n]othing in the present Charter shall impair the inherent right of individual and collective self-defense if an armed attack occurs against a Member of the United Nations.”⁹⁰ The *jus ad bellum* fundamentally seeks to constrain the resort to force between states.⁹¹ The *Tallinn Manual 2.0* extends these rules to cyber operations,⁹² specifying that a cyber operation is a use of force “when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”⁹³

4. Sovereignty/Unlawful Intervention

Even though a cyber-attack might not be severe enough to qualify as a use of force or armed attack, less-

⁸⁸ THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 1 (Dieter Fleck, ed., 2nd ed, 2008).

⁸⁹ MARCO SASSOLI, *Jus ad Bellum and Jus in Bello – The Separation between the Legality of the Use of Force and Humanitarian Rules to Be Respected in Warfare: Crucial or Undated*, in INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES, 241, 242 (Michael Schmitt & Jelena Pejic eds., 2007).

⁹⁰ UN Charter, *supra* note 87, art. 51.

⁹¹ *IHL and other legal regimes – jus ad bellum and jus in bello*, INTERNAT’L COMMITTEE OF THE RED CROSS (Oct., 29, 2010), <https://www.icrc.org/eng/war-and-law/ihl-other-legal-regimes/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm> (last visited Jan. 24, 2018).

⁹² TALLINN MANUAL 2.0, *supra* note 45, r.68.

⁹³ *Id.*, r.69.

severe operations might still violate international law as a violation of sovereignty or an unlawful intervention in the affairs of another state. The protection of sovereignty is noted in Rule 4 of *Tallinn 2.0*, which provides as follows: “[a] State must not conduct cyber operations that violate the sovereignty of another State.”⁹⁴ The Tallinn Manuals’ experts did not precisely delineate when a cyber operation would constitute a violation of sovereignty. At a minimum, a violation of sovereignty would occur when “when one State’s cyber operation interferes with or usurps the inherently governmental functions of another State.”⁹⁵ In addition, sufficient “infringement upon the target State’s territorial integrity”⁹⁶ would also qualify. While the degree necessary to constitute a sufficient infringement upon territorial integrity was not specified, the experts identified three levels of possible infringement: “(1) physical damage; (2) loss of functionality; and (3) infringement upon territorial integrity falling below the threshold of loss of functionality.”⁹⁷

The rule against intervention in the internal or external affairs of another State provides clearer contours and is considered a more serious violation of international law. Codified in the *Tallinn Manual 2.0*, Rule 66 states: “[a] State may not intervene, including by cyber means, in the external or internal affairs of another state.”⁹⁸ The experts identified this rule as being based on the principle of sovereignty and Articles 2(1), (3) and (4) of the UN Charter.⁹⁹ This rule carves out a *domaine réservé* left “solely

⁹⁴ *Id.*, r. 4.

⁹⁵ *Id.*, r.4, para. 15.

⁹⁶ *Id.*, r. 4, para. 10.

⁹⁷ *Id.*, r. 4, para. 11.

⁹⁸ *Id.*, r.66.

⁹⁹ *Id.*, r. 66, para. 1.

to the prerogative of States” and “regarded as protected from intervention by other States”¹⁰⁰ The most frequently cited formulation of the *domaine réservé* is “choice of a political, economic, social and cultural system, and the formulation of foreign policy.”¹⁰¹ Cyber-attacks which intrude on a nation-state’s *domaine réservé* would violate international law.

5. Conclusion

The above overview of both customary and treaty law demonstrates that significant work has been done and that a comprehensive international legal framework for cyber operations is currently in place. While challenges remain in governing this arena, they certainly are not due to a lack of legal provisions. That said, it is understandable that Smith might imply that a normative legal void exists necessitating a Digital Geneva Convention because of the number of cyber-attacks attributed to State actors as well as those acting as proxies for States. A review of the cyber operations cited by Smith will demonstrate both that there are substantive international law norms addressing these situations but will also begin to reveal the difficulties in enforcing that law.

C. Prominent Attacks and Attacks Cited by Smith—How They Fit into the Legal Framework

In his prelude to his proposal for a Digital Geneva Convention, Smith cited four instances of State cyber

¹⁰⁰ *Id.*, r.66, para. 7.

¹⁰¹ Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. V. U.S.), 1986 I.C.J. 14, para. 205 (June 27) [hereinafter *Nicaragua Judgement*].

operations: (1) the alleged Chinese theft of U.S. commercial secrets by Chinese military officers;¹⁰² (2) the North Korean hack of Sony;¹⁰³ (3) the Russian takedown of the Ukraine power grid;¹⁰⁴ and (4) the Russian influence of the U.S. 2016 presidential elections through the release of information damaging to Hillary Clinton in the DNC emails and John Podesta emails which they had hacked.¹⁰⁵ Of these incidents, only the Chinese hack is not already prohibited by international law, although individuals engaged in the hack were indicted for violating the U.S. domestic law. We will look at each incident in turn:¹⁰⁶

1. Sony/North Korea

The Sony cyber operation by North Korean proxy resulted in the deletion of significant amounts of data and the

¹⁰² Pierre Thomas & Mike Levine, *US Charges 5 Chinese Military Hackers in '21st Century Burglary*, ABCNEWS (May 19, 2014), <http://abcnews.go.com/US/us-charges-chinese-military-hackers-21st-century-burglary/story?id=23774172>. Smith showed this webpage on his slides while discussing this attack.

¹⁰³ Nakashima, Timber & Peterson, *supra* note 4.

¹⁰⁴ Jordan Robertson & Michael Riley, *How Hackers Took Down a Power Grid*, BLOOMBERG.COM (Jan. 14, 2016, 3:13 PM), <https://www.bloomberg.com/news/articles/2016-01-14/how-hackers-took-down-a-power-grid>. Smith showed this webpage on his slides while discussing this attack.

¹⁰⁵ *The John Podesta emails released by WikiLeaks*, CBS NEWS (Oct. 13, 2016, 4:42 PM), <https://www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/>. Smith showed this webpage on his slides while discussing this attack.

¹⁰⁶ Note that this analysis assumes that the attribution for the attack is correct, which is not necessarily a valid assumption. After a review of these hacks and the associated legal analysis, the following section will consider the difficulties that attribution poses to enforcing the existing legal regimes.

release of private information.¹⁰⁷ The data deletion and release of private information would also likely violate the sovereignty of the U.S. There are a couple of other points that should be made regarding this incident. The editor of the *Tallinn Manual 2.0*, Professor Michael Schmitt, indicated that such an operation, assuming that it could be attributed to the North Korean government, would in fact constitute a violation of U.S. sovereignty.¹⁰⁸ He would view the North Korean “manipulation of cyber infrastructure in another State’s territory” and “the emplacement of malware within systems located [in another State]” as violations of the target State’s sovereignty, and North Korea would be responsible for this internationally wrongful act.”¹⁰⁹

2. Russia/Podesta/DNC

In these two related instances, emails from both Jon Podesta and the Democratic National Committee which were damaging to the campaign of Hillary Clinton were released during the run-up to the 2016 U.S. presidential election. It appears that Podesta and the DNC were victims of a phishing email, which enabled malware to be downloaded to obtain the emails. While the emails were released through Wikileaks, the Obama administration publically attributed the operations to Russia and took measures in response to the attack, alleging that they were “intended to interfere with the US election process.”¹¹⁰ In

¹⁰⁷ Nakashima, Timber & Peterson, *supra* note 4.

¹⁰⁸ Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, Just Security, (Dec. 17, 2014), <https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/>.

¹⁰⁹ *Id.*

¹¹⁰ Press Release, Joint Statement of the Dept. of Homeland Sec. and

this instance, the hack appears to violate the prohibition on non-intervention in the affairs of another state, which is identified in Rule 66 of *Tallinn Manual 2.0*. This Rule implicates the concept of *domaine réservé*, those areas left “solely to the prerogative of States,”¹¹¹ of which elections would certainly qualify.¹¹² Note however, that the Obama Administration engaged in a “studied avoidance” on whether this cyber operation violated international law,¹¹³ although an administration attorney indicated that a cyber operation that “manipulates another country’s election results would be a clear violation of the rule of non-intervention.”¹¹⁴ While no reason was given for this “studied avoidance,” Professor Schmitt indicated that the reason was to avoid a comparable characterization of similar U.S. cyber operations.¹¹⁵ Despite the Obama Administration reluctance on this point, the administration allegation that Russian intended to influence the U.S. election would seem to imply that Russia violated the rule against non-intervention.

3. Russian Takedown of Ukraine Power Grid

In this situation, Ukrainian power stations were taken

Off. of the Dir. Of Nat’l Intelligence on Election Security, (Oct. 7, 2016), <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.

¹¹¹ TALLINN MANUAL 2.0, *supra* note 45, r.66, para. 7.

¹¹² See *id.*, r.66, para. 2 (citing an operation to alter electronic ballots as an example of a violation of the prohibition against non-intervention).

¹¹³ Ryan Goodman, *International Law and the US Response to the Russian Election Interference*, JUST SECURITY (Jan. 5, 2017), <https://www.justsecurity.org/35999/international-law-response-russian-election-interference/>.

¹¹⁴ *Id.* (quoting State Department Legal Advisor Brian Egan).

¹¹⁵ Schmitt, *supra* note 38, at 242-43 n. 5.

offline by an apparent hack by the Russian government or one of its non-State proxies.¹¹⁶ This operation on the electrical grid is just one of numerous attacks that Ukraine has suffered over the past three years, which have systematically undermined every aspect of Ukrainian society.¹¹⁷ These attacks appear connected with the current undeclared military conflict that is ongoing between Russia and the Ukraine, during which apparently Russian troops have facilitated the takeover of Crimea.¹¹⁸ The general thought is that Russia is trying to undermine the credibility of the Ukrainian government.¹¹⁹

This particular conflict demonstrates again the applicability of international law, but also the difficulty of attribution and enforcement. To the extent that the military actions in the Ukraine are attributable to Russia (which seems quite clear), Russia is in violation of the UN Charter's prohibition on the use of force and these accompanying cyber operations would also constitute a violation of the prohibition on the use of force.¹²⁰ In fact, Professor Schmitt has noted that Russia is deliberately obfuscating its role in order to take advantage of "grey zones" in international law.¹²¹ In addition, to the extent that the ongoing conflict is considered an international armed conflict (which is the

¹¹⁶ Robertson and Riley, *supra* note 104.

¹¹⁷ Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017, 6:00 AM), <https://www.wired.com/story/russian-hackers-attack-ukraine/>.

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ Thomas Grant, *Russia's Invasion of Ukraine: What does International Law have to Say?*, LAWFARE (Aug. 25, 2015, 7:45 AM), <https://www.lawfareblog.com/russias-invasion-ukraine-what-does-international-law-have-say>.

¹²¹ Michael Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 Yale J. of Int'l L. 1 (2017).

position of Amnesty International¹²²), these cyber-attacks would also be regulated by the Geneva Conventions. While a belligerent is authorized to target a dual-use facility (that is, a facility with both a civilian and military purpose),¹²³ such as the electrical power grid, such an attack must offer the party a definite military advantage and, in addition, the attack must be proportional—that is, the collateral damage must not be excessive in relation to the expected military advantage.¹²⁴ In this particular case, assuming an international armed conflict, if in fact Russia is targeting electrical facilities to undermine the Ukrainian government, such an attack would likely be prohibited under the law of armed conflict as this does not constitute a definite military advantage.

4. Chinese Hacking of U.S. Companies

The Chinese hacking of U.S. companies in order to engage in commercial espionage might not be unlawful under current international law, although it would certainly be a violation of U.S. domestic law. According to the article cited by Smith, the U.S. indicted five Chinese military officers for breaking into commercial networks and stealing secrets from U.S. nuclear, solar and metals industries.¹²⁵ This event was characterized by U.S. government officials as cyber espionage.¹²⁶ Rule 32 of *Tallinn 2.0* indicates that

¹²² *Ukraine: Mounting evidence of war crimes and Russian involvement*, AMNESTY INTERNAT'L (Sept. 7, 2014, 00:00 UTC), <https://www.amnesty.org/en/latest/news/2014/09/ukraine-mounting-evidence-war-crimes-and-russian-involvement/>.

¹²³ TALLINN MANUAL 2.0, *supra* note 45, r.101.

¹²⁴ *Id.*, r. 113

¹²⁵ Thomas & Levine, *supra* note 102.

¹²⁶ *See id.* (quoting Assistant Attorney General for National Security

cyber espionage “does not *per se* violate international law” although the method utilized to conduct espionage might violate international law.¹²⁷ In this situation, where there appears to be little adverse effect beyond the pilferage of commercial secrets, it is likely that this attack would not violate current international law. That said, as noted by Smith in his speech, the United States and China entered into a bilateral agreement not to engage in commercial cyber espionage.¹²⁸ As a result, subsequent actions might constitute a violation of this agreement.

D. A significant part of the problem: attribution

The foregoing discussion overlooks a glaring problem preventing a strong enforcement regime for violations of international law in cyberspace—the attribution of who conducted the attack. The inability to definitively attribute an attack to a particular State renders it difficult or impossible to even engage the limited enforcement mechanisms available under international law. This attribution problem has several aspects: (1) How does one definitively determine the individual or computer

John Carlin indicating that this theft is cyber espionage).

¹²⁷ TALLINN MANUAL 2.0, *supra* note 45, r.32.

¹²⁸ Smith, *supra* note 1. This agreement was noted in a White House press release. The substance of the agreement stated: “The United States and China agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.” Press Release, The White House, *Fact Sheet: President Xi Jinping’s State Visit to the United States*, (Sept. 25, 2015), <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

responsible for a particular attack?; (2) Even if one definitively identifies the individual responsible for an attack, how does one determine that the individual is operating on behalf of a State?; and (3) Even if a victim of a cyber-attack is able to definitively attribute the source of the attack to a State, how does the victim State provide proof of this fact without revealing its cyber and/or intelligence capabilities?

1. Determining the individual or system responsible.

The nature of the Internet renders this determination very difficult in practice. This fact is highlighted by the comments by then-candidate Trump about “somebody sitting on their bed who weighs 400 pounds” who could be responsible for the alleged Russian election interference hacks.¹²⁹ Addressing this concern implicates the privacy debate that has been ongoing for some time. In fact, many in the technology sector laud developments that enable individuals to remain anonymous, such as encryption and anonymous browsing on the TOR router. Features such as these allows individuals to organize and communicate without government interference—a good thing for the Arab Spring, not so much for child pornographers and terrorists. In the U.S. there has been a strong resistance from the technology sector to proposals to require encryption backdoors which would allow the government to decrypt and

¹²⁹ This statement was made during the first Presidential debate against Hillary Clinton. See Aaron Blake, *The first Trump-Clinton presidential debate transcript, annotated*, THE FIX (Sept. 26, 2016), https://www.washingtonpost.com/news/the-fix/wp/2016/09/26/the-first-trump-clinton-presidential-debate-transcript-annotated/?utm_term=.def6b520e2a2.

view any encrypted communication.¹³⁰ However, tools enabling privacy and confidentiality also make it very difficult for governments to identify individuals conducting cyber-attacks.

The privacy debate is an important one, and we do not mean to suggest that all privacy protections should be abolished in order to solve the attribution problem. Instead, the technology sector should consider the effects that privacy-friendly policies have on their fight against State-sponsored cyber operations. A Digital Geneva Convention would be toothless if States continue to be able deflect claims of responsibility because no single entity can be effectively identified as the source of a cyber operation.

2. Attributing an attack to a State

Even if a victim of a cyber-attack is able to identify the individual or group perpetrating the attack, the State from which the attacker operated is not necessarily responsible. If the individual is operating on his/her own, without direction, control, or at the instruction of a State, then international law is not necessarily implicated. The *Tallinn Manual 2.0* lays out circumstances when an attack may be attributed to a nation-state, and two are particularly relevant to this inquiry: (1) “Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority”;¹³¹ (2) “Cyber operations conducted by a non-State actor” when either “engaged in pursuant to [the State’s] instructions or under its

¹³⁰ Emblematic of this approach was Apple’s refusal to comply with an FBI subpoena to decrypt the cell phone from the San Bernardino shooters. See Tim Cook, *A Message to Our Customers*, (Feb. 16, 2016), <https://www.apple.com/customer-letter/>.

¹³¹ TALLINN MANUAL 2.0, *supra* note 45, r.15.

direction or control” or “the State acknowledges and adopts the operation as its own.”¹³²

If no conditions exist from which one may legally attribute an individual or group’s cyber-attack to a State,¹³³ then the individual may be liable for violating the law in either the State from which he is operating or the target state being attacked. Such an individual can be prosecuted under the host State’s laws or extradited to the victim state for prosecution. However, even the extradition process is difficult as States may refuse to extradite, as Russia has done for many Russian hackers indicted in the United States for violations of the Computer Fraud and Abuse Act.¹³⁴

3. Proving an attack

The previous two hurdles are significant, but assuming they can be surmounted, then the victim of a cyber operation must be able to demonstrate attribution in order to credibly invoke the enforcement mechanisms that international law provides. A State may not be willing to do

¹³² *Id.*, r.17.

¹³³ In addition to the possibility of formal attribution, a nation-state has a due diligence requirement to prevent cyber-attacks from cyber infrastructure within its borders or under its sovereign control. This requirement, however, is limited to requiring a state to take action to stop a cyber-attack when it has actual knowledge of the attack. Under this framework, a victim state must notify the state from which the attack is emanating and this state must take steps to stop the attack, otherwise the nation-state from which the attack is emanating is in violation of its international law due diligence obligations. See TALLINN MANUAL 2.0, *supra* note 45, r.4.

¹³⁴ Tim Lister and Tomas Etzler, *The US and Russia are fighting over the extradition of this hacking mastermind*, CNN (Nov. 26, 2017, 10:21 AM), <http://www.cnn.com/2017/11/25/europe/us-russia-extradition-fight/index.html>.

so, given that such an action may reveal that State's cyber capacities. International law does account for this difficulty, to a limited extent, in its rules permitting action in self-defense or countermeasures. States utilizing countermeasures need only utilize a reasonableness determination in order to execute countermeasures, but they are responsible for countermeasures that are made on a mistaken basis of attribution.¹³⁵ A similar reasonableness requirement exists for actions taken in self-defense.¹³⁶ That said, a State will likely desire to state its case to the international community, as the FBI did in attributing the Sony hack to North Korea.¹³⁷

The attribution problem presents an opportunity for the technology sector to provide its expertise and develop a reputation as a trusted neutral party. The technology sector can analyze its data on attacks, in conjunction with information that States are willing to provide it, and make independent attribution assessments. To the extent that they would be able to build and retain a reputation for trustworthiness and neutrality, they could provide important input to the process and improve the ability of States to enforce the current legal framework. In addition, such a process might work in the long run towards States being willing to agree to a multilateral treaty regime that Smith proposes.

¹³⁵ TALLINN MANUAL 2.0, *supra* note 45, r.20, para. 15.

¹³⁶ *Id.*, r.71, para. 23.

¹³⁷ Press Release, FBI National Press Office, Update on Sony Investigation (Dec. 19, 2014), <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> .

II. STATES ARE UNLIKELY TO AGREE TO SMITH'S PROPOSED
DGC WHICH LIMITS THEIR CYBER OPERATIONS

Notwithstanding the fact that there are significant international law provisions applicable to cyber operations, there is another critical point that Smith must consider when seeking to achieve the goal of a Digital Geneva Convention: will States agree to join and abide by such a treaty? In the case of the UN Charter and the Geneva Conventions, States affirmatively agreed to join these multi-lateral treaties and give their provisions legal effect. These “laws” were not imposed by a super-legislature of States, nor by some other outside authority. To the extent that custom also developed over time, States could be persistent objectors to a developing custom and the State would not be legally bound.¹³⁸

This raises a key question: Why do States agree to legal obligations in the first place? There are many scholarly theories and discussions on why a State agrees to assume a legal obligation, but the issue boils down to whether a State views the assumption of such an obligation as being in its best interest.¹³⁹ That is, the prospective perceived benefits of joining the treaty regime must outweigh the perceived costs of assuming the legal obligation.

The fundamental problem, then, that Smith faces is that he has to be able to persuade the States that are allegedly using cyberspace to conduct operations—Russia, China, United States, Israel, Iran, and North Korea among many others—to agree to substantial limits on their ability to

¹³⁸ See ILA CUSTOMARY LAW PRINCIPLES, *supra* note 31, principle 15. This principle provides that “[i]f whilst a practice is developing into a rule of general law, a State persistently and openly dissents from the rule, it will not be bound by it.” *Id.*

¹³⁹ MARK WESTON JANIS, INTERNATIONAL LAW, 12-14 (5th ed., 2008).

conduct cyber operations. In order to do so, Smith has to be able to answer a number of questions:

-Why is it in these States' best interest to agree to these limits?

-How can they be assured that others will comply? How can a State be reasonably certain that other States will comply especially considering the highly secretive nature of cyber operations as well as the fundamental problem of attribution? As a corollary, how would these legal provisions be enforced?

-How can these legal provisions be enforced when it's so difficult to attribute a cyber operation to a particular State?

Smith and other proponents of the Digital Geneva Convention fail to answer the question of why it would be in the best interest of the States to agree to such legal restrictions. In fact, Professor Schmitt argues that the opposite is occurring—that States are taking advantage of “grey zones” in international law in order to conduct cyber operations.¹⁴⁰ Before addressing the issue of consent as it applies to cyber, it will be helpful to consider why States agreed to the *jus in bello* and *jus ad bellum* codified in the Geneva Conventions and UN Charter respectively. From this starting point, we can examine the potential reasons for States to agree to additional significant legal restrictions and obligations. This article will now turn to examine the origins of these bodies of law to help answer that question.

¹⁴⁰ Schmitt, *supra* note 121, at 2-3.

A. *Consent and the Geneva Conventions and UN Charter*

When examining the origins of the Geneva Conventions and UN Charter, it is important to keep in mind that they were adopted shortly after the world experienced the horrors of the Second World War and the commencement of the nuclear age. In fact, the 1949 Geneva Conventions represent the first time in modern history an international treaty has achieved universal acceptance,¹⁴¹ whereby all States in the world agree to the protections it affords to the victims of war. Similarly, the UN Charter's prohibition on the use of force and the *jus ad bellum* framework have been widely accepted, to the extent that the International Court of Justice has stated that it constitutes customary law.¹⁴² While World War Two may have served as the impetus for the adoption of these treaties, there are several reasons why it is within a State's best interest to adhere to these legal bodies of law.

From a practical point of view, compliance with the law of armed conflict promotes military effectiveness. For example, pursuant to the Third and Fourth Geneva Conventions, States involved in an international armed conflict are to treat prisoners of war and protected persons humanely and in accordance with the obligations detailed within those two conventions.¹⁴³ The practical effect of this

¹⁴¹ Press Release, Internat'l Committee of the Red Cross, Geneva Conventions of 1949 achieve universal acceptance, (Aug. 21, 2006), <https://www.icrc.org/eng/resources/documents/news-release/2009-and-earlier/geneva-conventions-news-210806.htm>.

¹⁴² *Nicaragua Judgement*, *supra* note 101, para. 188.

¹⁴³ Under the Fourth Geneva Convention, article 4, protected persons are defined as follows: "[p]ersons protected by the Convention are those who, at a given moment and in any manner whatsoever, find

is twofold: (1) Members of the respective armed forces will not feel compelled to “fight to the death” because they will be confident that they will be treated humanely upon capture by their adversary; (2) it will ultimately be easier for the parties to the conflict to end the hostilities. The reverse of this is also true. If during an armed conflict, the parties to the conflict intentionally violate the law of armed conflict by doing things like -- targeting civilians and civilian objects, or mistreating prisoners of war and protected persons – it will likely prolong a conflict.

Compliance with the law of armed conflict also increases the likelihood of reciprocity among nations. If one party to an armed conflict abides by the laws of armed conflict, it may serve to encourage or facilitate their adversaries to act in the same or similar way. Of course, there is not a guarantee this will happen. It is also important to note that the law of armed conflict is not based upon reciprocity. Common article one to the 1949 Geneva Conventions provides “[t]he High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.” Put in a slightly different manner, States are required to comply with their obligations regardless of what their adversaries do. But, as a practical matter, if you treat the other side’s prisoners inhumanely and target civilians and civilian objects, one cannot be too surprised if

themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals. Nationals of a State which is not bound by the Convention are not protected by it. Nationals of a neutral State who find themselves in the territory of a belligerent State, and nationals of a co-belligerent State, shall not be regarded as protected persons while the State of which they are nationals has normal diplomatic representation in the State in whose hands they are.” Geneva Convention relative to the Protection of Civilian Persons in Time of War art. 4, Aug. 12, 1949, 75 U.N.T.S. 287

the other side does the same or similar things.

Also, there is a significant reputational cost for failing to comply with both the law of armed conflict and the *jus ad bellum*, both internationally and domestically. One need only think about incidents of Abu Gharib or the My Lai massacre. The loss of legitimacy associated with engaging in such conduct has practical consequences. For example, after 9/11, organs and agents of the United States mistreated a number of the prisoners it held in the so-called war on terrorism. Some of this maltreatment included the actual torture of prisoners. Unquestionably, this conduct stained the reputation of the United States and its armed forces and intelligence agencies. The practical effect of such conduct is that it made other countries, in some cases, reluctant to operate with the United States. Also, as a practical matter, it makes it very difficult to prosecute individuals that were physically and mentally coerced or otherwise subject to torture or cruel, inhumane, or degrading treatment. This type of conduct undermines the position of the United States internationally especially from a morality or rule of law perspective. With respect to the impact domestically, violations of the law of armed conflict undermine a war effort. It helps galvanize support against involvement in an armed conflict. Again, the massacre at My Lai during the Vietnam War is an example of an incident that helped erode domestic public support for the conflict.

From a humanitarian perspective, armed conflict is not intended to be a bloodsport. In fact, the modern law of armed conflict has largely been driven by humanitarian concerns and pressures.¹⁴⁴ As noted by Professor Gary Solis, “[t]he idea of war as indiscriminate violence suggests violence as an end in itself, and that is antithetical to the fact

¹⁴⁴ SOLIS, *supra* note 25, at 8.

that war is a goal-oriented activity directed to attaining political objectives.”¹⁴⁵ Additionally, war victims on all sides of a conflict are not responsible for the fact that their State decided to fight an armed conflict.¹⁴⁶ Even from a humanitarian perspective, it is important to highlight that the law of armed conflict is a body of law that, even at its very best, is never more than imperfectly observed and, at its worse, is very poorly observed.¹⁴⁷ Commenting on the laws regulating warfare, British historian Geoffrey Best stated “[i]ts mission, strictly speaking, is impossible. It seeks to introduce moderation and restrain into a medium peculiarly insusceptible to those qualities.”¹⁴⁸ Coming full circle, States agree to the Geneva Conventions and the use of force prohibitions contained in the U.N. Charter to mitigate the harshness and brutality of warfare. That is, the law of armed conflict “has done nothing but good, and the implication is clear, that wars where it was not enforced, known, or even dimly apprehended, were the most horrible for their lack of it.”¹⁴⁹

*B. Breakdown of Government Group of Experts
Process: Not a Good Start*

The prospects of developing a universally-accepted Digital Geneva Conventions were significantly diminished by the recent actions of the UN Government Group of Experts (hereafter GGE).¹⁵⁰ The breakdown or collapse of

¹⁴⁵ *Id.*

¹⁴⁶ MARCO SASSÒLI, ANTOINE A. BOUVIER & ANNE QUINTIN, HOW DOES LAW PROTECT IN WAR? 119 (2011).

¹⁴⁷ GEOFFREY BEST, HUMANITY IN WARFARE 11 (1980).

¹⁴⁸ *Id.*

¹⁴⁹ *Id.* at 12.

¹⁵⁰ Schmitt & Vihul, *supra* note 62.

the processes was generally along Cold War lines with States like Cuba, Russia and China rejecting the final report due to three additions to a list of cyber-relevant legal principles and rules that had been originally agreed to by the experts in 2015.¹⁵¹ Specifically, these nations objected to statements affirming States' ability to act in self-defense in cyberspace and to utilize countermeasures in response to internationally wrongful acts committed in cyberspace.¹⁵² Finally, these nations objected to a statement affirming the applicability of the law of armed conflict in cyberspace.¹⁵³ Unlike the universally agreed-upon norms protecting the victims of war espoused in the 1949 Geneva Conventions, it is hard to ignore the fact that, as noted by Professor Schmitt and Liis Vihul, even well-accepted international legal norms have been intentionally politicized.¹⁵⁴ It is not entirely clear why Cuba, Russia, and China took such untenable political positions on the above issues even though they have accepted the general applicability of international law to cyberspace and operations.¹⁵⁵ Schmitt and Vihul have speculated that their positions may be rooted in a desire to avoid the perception that the "the West" is disproportionately prescribing the principles and the rules governing cyberspace.¹⁵⁶ Alternatively, these recalcitrant States, particularly Russian and China, may be viewing their position through a legal-operational lens of wanting to deprive the United States and its Western allies of a legal justification for responding to their hostile cyber

¹⁵¹ *Id.*

¹⁵² *Id.*

¹⁵³ *Id.*

¹⁵⁴ *Id.*

¹⁵⁵ *Id.*

¹⁵⁶ *Id.*

operations.¹⁵⁷ Finally, “opposition to acknowledging basic and irrefutable legal notions may reflect the current dismal state of relations outside the cyber realm. These may be ‘softball’ legal issues, but right now everyone is playing ‘hard ball.’”¹⁵⁸

The dynamics –legal, political, and practical-- underpinning the failure of the U.N. GGE powerfully illustrate why the notion of reaching broad international consensus on a Digital Geneva Convention for Cyberwarfare is not only infeasible but highly unlikely. Some of the most direct fault lines and frictions between States exist in the cyber domain. Is the United States going to forgive Russia for interfering in its 2016 elections? China has pillaged intellectual property from American companies through cyber espionage for decades resulting in the greatest transfer of wealth in human history.¹⁵⁹ It is difficult to overstate the negative impact that such theft has had on American economic growth and prosperity and the ways in which it has undermined America’s military and national security.¹⁶⁰

In addition and related to the intractable nature of the international and political dynamics mentioned above, as a practical matter, most of the States that are particularly advanced and active with cyber operations would not be interested in entering into a Digital Geneva Convention. Cyber operations are among the most sensitive, highly classified secrets held by States. In many respects, “[t]he entire phenomenon of cyber war is shrouded in such

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ Dennis Blair & Keith Alexander, *China’s Intellectual Property Theft Must Stop*, N.Y. TIMES (Aug. 15, 2017), <https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html>.

¹⁶⁰ *Id.*

government secrecy that it makes the Cold War look like a time of openness and transparency.”¹⁶¹ Unlike conventional and even nuclear weapons and warfare, everything related to cyber warfare is enveloped in extreme secrecy.¹⁶² Not to overstate a point, there are certainly many aspects of nuclear weapons that are highly classified: specifics about design and capabilities; launch codes; targeting plans; and command and control among many other tactical, operational, and strategic details.¹⁶³ But, in comparison to cyber weapons, there is much that is publicly known and widely understood about nuclear weapons and warfare such as how many particular States have at any given time; how they generally work; and the terrifying reality of what happens when they are used.¹⁶⁴

C. Proposal for a cyber International Atomic Energy Agency presumes a robust treaty regime for enforcement—might be helpful but still requires consent.

Despite the difficulties identified above, there is merit to Mr. Smith’s idea of an international, independent watchdog agency like the International Atomic Energy Agency (hereinafter IAEA). However, even such an organization requires State consent to a multi-lateral treaty. The IAEA is comprised of member States who have ratified the Statute of the IAEA,¹⁶⁵ a multi-lateral treaty establishing

¹⁶¹ RICHARD A. CLARKE, CYBER WAR xi (2010).

¹⁶² FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 284 (2016).

¹⁶³ *Id.*

¹⁶⁴ *Id.*

¹⁶⁵ Statute of the International Atomic Energy Agency, July 29, 1957, 276 U.N.T.S. 3 [hereinafter IAEA Statute].

the IAEA which 169 nation-states have ratified.¹⁶⁶ The IAEA Statute specifies the functions of the IAEA, which is primarily focused on research, development and safety in the development of peaceful uses of nuclear energy.¹⁶⁷ The IAEA is governed by the General Conference, comprised of all Member States, and the Board of Governors, which has a rotating membership of 35 Member States.¹⁶⁸ While much of the public face of the IAEA consists of the technical experts who conduct inspections and issue reports, it cannot be forgotten that their work is also overseen by the Member States to the Statute of the IAEA. In addition, it should be noted that the Statute of the IAEA does not address nuclear nonproliferation. This topic is addressed by the Treaty on The Non-Proliferation of Nuclear Weapons, which specifies that the IAEA will work with States subscribing to the Non-Proliferation Treaty to ensure that peaceful nuclear energy programs do not divert materials to developing nuclear weapons.¹⁶⁹ The work of the IAEA, then, is a verification mission, not an enforcement mission. Enforcement is left to States, usually working through the United Nations.

Smith's proposal of an IAEA-like structure might be a helpful first step in the process of more robust international law framework for cyber operations. Note that the Statute of the IAEA entered into force in 1957, fairly soon after the start of the nuclear age. While the dangers of nuclear

¹⁶⁶ *List of Member States*, IAEA, <https://www.iaea.org/about/governance/list-of-member-states> (last visited Jan. 19, 2018)

¹⁶⁷ See IAEA Statute, *supra* note 165, art.3 (specifying functions of the IAEA).

¹⁶⁸ *Id.*, arts. 5-6.

¹⁶⁹ See Treaty on the Non-proliferation of Nuclear Weapons, art. 3, July 1, 1968, 729 U.N.T.S. 161 [hereinafter Nuclear Non-proliferation Treaty].

weapons were clear at that time, this Statute did not attempt to address substantive issues such as non-proliferation and nuclear weapons disarmament, which would have been non-starters at that time.¹⁷⁰ Instead, the Statute focused on peaceful uses of nuclear energy and standards for nuclear safety.¹⁷¹ This foundation allowed IAEA to assist in the implementation of the Non-Proliferation Treaty when it entered into force in 1970, overseeing the peaceful development of nuclear energy to ensure that nuclear materials were not then diverted to weapons development.¹⁷² A similar process in the case of cyber might be to create a similar organization to promote peaceful development of the global network and promote safety and security. That said, while there is a clear demarcation between peaceful and non-peaceful uses of nuclear energy, there is not a similar clear-cut line in the cyber arena as the range of uses of cyberspace is much more varied than nuclear energy. Despite this fact, an independent agency that begins to analyze and discuss issues related to cyber security would be a helpful first step.

The bottom line conclusion in response to Smith's call for an "independent watchdog" akin to the IAEA, is that, much like the prospects of a multi-lateral treaty, States would have to consent to such an agency in order for it to have any enforcement teeth. Given the dynamics addressed earlier and the dim prospects of a widely-accepted multilateral treaty regarding cyber, a similar resistance by States should be expected in response to this proposal.

¹⁷⁰ See IAEA Statute, *supra* note 165, art.3 (specifying functions of the IAEA).arp

¹⁷¹ *Id.*

¹⁷² Nuclear Non-proliferation Treaty, *supra* note 169, art. 3.

III. THE TECH SECTOR COULD ASSIST IN THE DEVELOPMENT OF INTERNATIONAL LAW AS IT APPLIES TO CYBER

A. Develop a reputation as a trusted agent—this could serve as a platform for ongoing discussion and debate on the development of cyber operations law.

In Smith's speech, he proposes that the technology sector serve as a "digital Switzerland," committed to 100% defense and 0% offense. This analogy might be a little inaccurate—the idea of a Switzerland conveys the picture of a neutral state in a belligerency, which implies an entity remaining "above the fray," studiously avoiding assisting any of the belligerent parties. By emphasizing the degree to which the technology sector is on the "front lines," Smith's digital Switzerland analogy begins to break down.

A better analogy might be to the International Committee of the Red Cross (ICRC). The ICRC has been a critical component to the development and functionality of the law of armed conflict. The ICRC was present at the adoption of the four Geneva Conventions and has enjoyed a unique status under the law.¹⁷³ Part of their effectiveness is due to the fact that the ICRC has developed a reputation as a trusted agent, working directly with all parties to a conflict with the goal of advancing the cause of humanity in warfare without regard to the identity of the parties involved.¹⁷⁴ This model might be a better model for the technology sector to

¹⁷³ GCI, *supra* note 74, art. 9; GCII, *supra* note 74, art. 9; GCIII, *supra* note 74, art. 9; GCIV, *supra* note 74, art. 10.

¹⁷⁴ See *Building Respect for the Law*, INT'L COMM. OF THE RED CROSS (Jan. 5, 2011), <https://www.icrc.org/eng/what-we-do/building-respect-ihl/overview-building-respect-ihl.htm> (noting their outreach efforts to military and police units and armed groups fighting their governments).

attempt to emulate. As noted in Smith's speech, the technology sector is on the front lines on a regular basis and, as a result, has a unique ability to provide a helpful perspective to shape the development of the law. With the right leadership, cooperation from the largest global technology leaders, and a good-faith commitment to eliminating the weaponization of the Internet, the technology sector could create an entity like the ICRC to engage in the discussion and promote its vision of the internet.

B. Join the international law dialogue with a correct understanding of the state of the law and how international law is developed.

As has been discussed much within this article, there are significant efforts to address the international law issues associated with cyberspace. However, these efforts are largely the product of government officials, military officials and academics, not technology industry leaders. To date, there has been minimal participation from technology industry leaders. For example, the *Tallinn Manual 2.0* seven-page list of International Group of Experts and Other Participants includes only one individual who is affiliated with the technology industry.¹⁷⁵ Similarly, the list of participants from the 2013 and 2015 UN GGE reports is also devoid of technology industry representatives.¹⁷⁶

To address this void, the technology industry must inject itself into the process. They bring an expertise and front-line perspective that will help all parties understand the

¹⁷⁵ TALLINN MANUAL 2.0, *supra* note 45, at xviii. That individual is Jeffrey Carr, who is listed as being affiliated with Taia Global Inc.

¹⁷⁶ See 2015 GGE Report, *supra* note 64, annex; 2013 GGE Report, *supra* note 64, annex.

issues involved. However, instead of broad-brushed calls for a new treaty, the industry must appreciate the nuance and challenges presented by international law attempts to regulate this field. First, the industry must have an appreciation of the current state of customary law, as reflected by *Tallinn Manuals* and the GGE reports. Indeed, this lack of understanding is exposed by the fact that most of the cyber-attacks cited by Smith are addressed (albeit imperfectly) by the current legal framework. This understanding would lay the framework for progress on two additional fronts: (1) understanding the current “grey zones” in the law where the law does not adequately address the technological developments (and how some nation-states may use these grey-zones to their advantage); and (2) understanding the inherent limits of the enforceability of international law and the degree to which the lack of attribution renders the enforcement of the current legal framework even more difficult than normal. Second, the industry must have an appreciation of the degree to which the principle of state consent underlies the international law system. As stated earlier, to have a State sign a treaty limiting its options in cyberspace requires that the State view adopting the treaty as being in its national interest. Few States take this view as to date it is clear that States are taking advantage of gray zones to maximize flexibility in their cyber operations. Similarly, the development of customary law norms requires the same consideration, lest States reject developing customary norms as persistent objectors.

Part of the process that the technology sector can engage with is the development of customary law. While the authors of the Tallinn Manual were very careful to report on custom as it currently exists (*lex lata*, or existing law), and to avoid engaging in advocacy as to what the law should be

(*lex ferenda*),¹⁷⁷ there is a place for advocacy of *lex ferenda* by outside organizations. This can result in the consequent adjustment of customary law as state practice shifts in response to such calls for such changes.¹⁷⁸ The technology sector is in an ideal position to engage in *lex ferenda* advocacy based on their unique perspective. Indeed, there are models for the technology industry to consider as they enter the field. There are accepted models of establishing new customary norms through indirect means such as the establishment of soft law norms.¹⁷⁹ For example, codes of best practices, industry standards or aspirational norms can be defined, which may be adopted by individuals, corporations and/or States.¹⁸⁰ Over time, such best-practices or standards may gain widespread acceptance among States to the point where they evolve beyond soft-law aspirational guidelines and are cemented as hard-law customary law.¹⁸¹

In fact, Smith's proposal for the technology sector pledge could be characterized as a soft law norm. Smith advocates that the global technology sector sign its own pledge to the following terms: 1. No assistance in offensive actions; 2. Collaborative proactive defense; 3. Collaborative remediation after attacks; 4. Software patches made available to all; 5. Coordinate disclosure practices for vulnerabilities; 6. Support for intergovernmental defensive

¹⁷⁷ See *supra* note 55, and accompanying text.

¹⁷⁸ GERHARD VON GLAHN AND JAMES LARRY TAULBEE, *LAW AMONG NATIONS: AN INTRODUCTION TO PUBLIC INTERNATIONAL LAW*, 44-46 (10th ed. 2013).

¹⁷⁹ *Id.* at 68-69.

¹⁸⁰ *Id.*

¹⁸¹ See, D.J. Bederman, *Constructivism, Positivism, and Empiricism in International Law*, 89 *Georgetown L. Rev.* 469, 484 (reviewing ANTHONY CLARK AREND, *LEGAL RULES AND INTERNATIONAL SOCIETY* (2001)).

efforts.¹⁸² Such a pledge, if carried out effectively, would be significant towards the beginning of a soft-law norm and also might assist in establishing the technological sector as a trusted agent in the process. The process of developing soft-law norms is generally time-consuming, indirect and not always successful, but would provide a real road-map to industry engagement in the development of customary norms for cyber operations.

IV. CONCLUSION

Because companies like Microsoft and those similarly situated are on the front lines, as Brad Smith notes, it is understandable that they would perceive a significant problem from the increased number of State-sponsored cyber-attacks. Enforcement of international law is handicapped due to the difficulties discussed above and States taking advantage of gaps in the law in order to advance their national interests. It is understandable why Smith might perceive there to be a void in the legal framework, but this perception is not quite accurate. The international legal community should welcome the technology sector's involvement, and perhaps the joint efforts of these two groups working in concert might create a better functioning legal framework that meets the needs of States and the technology sector.

¹⁸² Smith, *supra* note 1.