KNOWN UNKNOWNS: STATE CYBER OPERATIONS, CYBER WARFARE, AND THE *JUS AD BELLUM*

PETER Z. STOCKBURGER*

> [T]here are known knowns: there are things we know we know. We also know there are known unknowns: that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know.

- Donald Rumsfeld, 2002[1]

I. INTRODUCTION

Over the past ten years, the advent of new and networked technology has had a tremendous impact on the geopolitical landscape. From the use of social media during the 2011 Arab Spring by activists to communicate their actions, to the use of hashtag campaigns to raise awareness about often ignored humanitarian crises,[2] networked technology has had an indelible impact on our collective social and political lives.

Over the past ten years, States have also increased their use of networked technology to further their offensive and defense

*Peter Z. Stockburger is a Managing Associate at Dentons U.S. LLP and an Adjunct Professor at the University of San Diego School of Law. The views and opinions stated herein belong to the author only, and are not reflective of either Dentons U.S. LLP, Dentons, or the University of San Diego School of Law.

1. Donald H. Rumsfeld, Secretary of Defense, Department of Defense News Briefing (Feb. 12, 2002).

2. *See generally* BRING BACK OUR GIRLS, HTTP://WWW.BRINGBACKOURGIRLS.US (LAST VISITED AUG. 15, 2016) (addressing Boko Haram's kidnapping of over 200 school girls in Nigeria); INVISIBLE CHILDREN: KONY 2012, HTTP://WWW.INVISIBLECHILDREN.COM/KONY-2012/ (LAST VISITED AUG. 15, 2016) (addressing the atrocities committed by the Lord's Resistance Army).

operational goals. States have developed "both formal and informal mechanisms for countering" the "rapidly developing threats and operations in cyberspace,"[3] including developing the United States (US) Cyber Command, China's People's Liberation Army General Staff Department's 3rd and 4th Departments,[4] Iranian Sun-Army and Cyber Army,[5] Israel's Unit 8200,[6] and the Russian Federal Security Service's Federal Agency of Government Communications and Information.[7] State conflict is now inextricably intertwined with networked technology.

In 2007, for example, Estonia was hit with a widespread distributed denial of service (DDoS) attack that shut down and defaced certain websites of Estonian government institutions and banks.[8] It was largely suspected that Russia had carried out the attack, although Russia denied any wrongdoing.[9] In 2008, Georgia suffered a similar attack when its critical infrastructure was hit with a DDoS attack, followed by a Russian-led kinetic operation in South Ossetia.[10] Due to the timing and structure of the attack, Russia was also suspected as the culprit (although it again denied any wrongdoing).[11] And in 2010, the world was introduced to Stuxnet, a computer virus that destroyed centrifuges inside Iran's Natanz uranium enrichment site, and infected industrial control systems

3. Laurie R. Blank, *Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 77 (Jens David Ohlin et al. eds., 2015).

4. *Id.* at 77 (citing LARRY M. WORTZEL, THE CHINESE PEOPLE'S LIBERATION ARMY AND INFORMATION WARFARE (2014)).

5. *Id.* (citing Tom Gjetlen, *Could Iran Wage a Cyber War on the U.S.?*, NAT'L PUB. RADIO, Apr. 26, 2012, http://www.npr.org/2012/04/26/151400805/could-iran-wage-a-cyberwar-on-the-u-s.).

6. *Id.* (citing Yaakov Katz, *IDF Admits to Using Cyber Space to Attack Enemies*, JERUSALEM POST, June 3, 2012).

7. *Id.* (citing *FAPSI Operations*, GLOBALSECURITY.ORG, http:www.globalsecurity.org/intell/world/russia/fapsi-ops.htm (last visited Aug. 15, 2016); RIA Novosti, *Russia to Create Cyberwarfare Units by 2017*, SPUTNIK, Jan. 30, 2014, http://en.ria.ru/military_news/20140130/187047301/Russia-to-Create-Cyberwarfare-Units-by-2017.html).

8. *See Estonia hit by 'Moscow cyber war'*, BBC NEWS, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

9. *See id.*

10. *See Marching off to cyberwar*, ECONOMIST, Dec. 4, 2008, http://www.economist.com/node/12673385.

11. *See id.*

worldwide. The scope and complexity of the Stuxnet virus led many observers to believe Israel and the US were involved. In 2012, the New York Times reported that Stuxnet was developed during the George W. Bush administration, and during the early years of the Obama administration, and was named "Operation Olympic Games."[12] In February 2016, the New York Times also revealed that Stuxnet was one element of a much larger prepared cyber attack by the US that would have targeted Iran's air defenses, communications systems, and key parts of its power grid.[13] That larger attack, dubbed "Nitro Zeus," was intended to be carried out in the event the diplomatic negotiations between the US (as part of the P-5) and Iran concerning Iran's nuclear development plans failed.[14]

This increase in State directed and approved cyber operations raises two critical questions: (1) what norms of international law apply to State directed or approved cyber operations, and (2) how? In 2011, the US recognized that the "development of norms for State conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. [Instead,] long-standing international norms guiding State behavior - in times of peace and conflict - also apply in cyberspace."[15] But the "unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."[16]

In 2009, the North Atlantic Treaty Organization's ("NATO") Cooperative Cyber Defence Centre of Excellence ("CCD COE") attempted to answer these questions by inviting an independent "International Group of Experts" ("IGE") to produce a manual on the international norms governing State use of cyber operations.[17] That

12. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

13. David E. Sanger & Mark Mazzetti, *U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict*, N.Y. TIMES, Feb. 16, 2016, http://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html.

14. *See id.*

15. WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011).

16. *Id.*

17. INT'L GRP. OF EXPERTS AT THE INVITATION OF THE NATO COOP. CYBER

manual, published in 2013, was entitled the MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, or as is more commonly known the TALLINN MANUAL. The TALLINN MANUAL set forth ninety-five "black letter rules" governing "cyber warfare," including discussion on topics such as sovereignty, State responsibility, the *jus ad bellum*, international humanitarian law (or the *jus in bello*), and the law of neutrality.[18]

One of the challenges States face in the cyber environment "is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent."[19] And "there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal regime."[20] As the principal author of the TALLINN MANUAL, Professor Michael N. Schmitt, explained, "uncertainty regarding the precise legal parameters of cyber warfare" continues to persist, and a "turbulent period should be expected *vis-à-vis* the law of cyber warfare as current international legal norms adjust to the changing national interests of states in cyberspace."[21]

This article focuses on the narrow issue of whether and to what extent the *jus ad bellum*, or the body of international law regulating when States may use force, applies to State directed or approved cyber operations. To that end, this article examines the conclusions of the TALLINN MANUAL with regard to the *jus ad bellum*, and seeks to identify any known unknowns that remain, including:

- What level of attribution should be required to impose State responsibility for a cyber operation?
- What type of cyber operation constitutes a "use of force" as prohibited under Article 2(4) of the United Nations (UN) Charter and customary international law?
- Are there types of coercive cyber attacks that are permissible under international law?
- What type of cyber attack constitutes a "threat of force" as

DEF. CTR. OF EXCELLENCE, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

18. *See generally id.*

19. *Id.* at 3.

20. *Id*.

21. Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis*?*, 25 STAN. L. & POL'Y REV. 269, 271, 273 (2014) [hereinafter Schmitt, *Cyber Warfare*].

prohibited under Article 2(4) of the UN Charter and customary international law?
- What type of cyber attack constitutes an "armed attack" as contemplated under Article 51 of the UN Charter and customary international law?
- Can cyber operations be utilized in exercising peremptory self-defense (assuming the doctrine of peremptory self-defense is recognized under customary international law)?
- Is cyber "humanitarian intervention" permissible?

Part II of this article discusses the relevant terminology governing this debate, including the types of cyber operations often used by States and the basic principles of the *jus ad bellum*. And Part III examines the conclusions of the TALLINN MANUAL as it pertains to the application of the *jus ad bellum*, and identifies what, if any, known unknowns remain.

II. THE ROLE OF RHETORIC - GETTING THE TERMINOLOGY RIGHT

The "greatest hindrance to effective conversation between cyber norm communities is terminological in nature."[22] The phrases "cyberspace," "cyber operations," "cyber warfare," and "cyber attacks" are often used by scholars, policymakers and journalists interchangeably and without distinction. This loose rhetoric can lead to overly broad responses and bad policy:

> The word "cyber" has grabbed the world's attention over the past several years: put "cyber" in front of nearly any word and you have a new term for a new millennium. In the media and public discourse, words such as cyber attack, cyberwar, cyber doom, cyber security, and cybercrime sell news and produce entirely new channels for debate and analysis. [. . .] [Cyberspace] is also fertile ground for runaway rhetoric - discourse and terminology that can have unintended effects reverberating far beyond the news story or journal attack.[23]

Understanding the rhetoric underlying the "cyber" debate therefore requires an understanding of: (1) the terminology used by State actors; (2) the types of operations being carried out by States;

22. Michel N. Schmidtt & Liis Vihul, *The Nature of International Cyber Norms, Tallinn Paper No. 5*, CCDCOE, at 6 (2014), https://ccdcoe.org/multimedia/tallinn-paper-nature-international-law-cyber-norms.html.

23. *See* Blank, *supra* note 3, at 76.

and (3) the international norms commonly understood to populate the *jus ad bellum* - namely the principles of non-intervention (including the prohibition against the use of force and the doctrine of collective and individual self-defense) and State responsibility.

A. CYBER TERMINOLOGY

1. CYBERSPACE

The Internet and its connected networks are often referred to as "cyberspace." Merriam-Webster defines "cyber" as "of, relating to, or involving computers or computer networks as the Internet."[24] Inter-governmental organizations and States generally define "cyberspace" broadly, including "hardware, software and information systems, [and] also people and social interaction within these networks."[25] The International Organization for Standardization, for example, defines "cyber" as "the complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."[26] The United Kingdom ("UK") has adopted a definition of "cyberspace" that includes "an interactive domain made up of digital networks that is used to store, modify, and communicate information."[27] And in its 2015 War Manual, the U.S. Department of Defense ("DOD?) defined "cyberspace" as a "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[28]

24. *Cyber*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/cyber (last visited Aug. 15, 2016).

25. NATIONAL CYBER SECURITY FRAMEWORK MANUAL 8 (Alexander Klimburg ed., 2012).

26. *Information Technology - Security Techniques - Guidelines for Cybersecurity,* INT'L ORG. FOR STANDARDIZATION & INT'L ELECTROTECHNICAL COMMISSION 4.21, https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (last visited Aug. 15, 2016).

27. THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD 11 (2011).

28. OFF. OF GENERAL COUNSEL DEP'T OF DEFENSE, DEP'T OF DEFENSE LAW OF WAR MANUAL § 16.1.2 (2015) [hereinafter LAW OF WAR MANUAL].

2. CYBER OPERATIONS

Cyber operations can be understood to include operations "against or via a computer or a computer system through a data stream."[29] Such operations aim to do different things, such as "infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system."[30] In its 2015 War Manual the US DOD defines "cyber operations" as those involving the "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace,"[31] including those that "use computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves[.]"[32] According to the US DOD, "cyber operations" can also be a "form of advance[d] force operations, which precede the main effort in an objective area in order to prepare the objective for the main assault."[33] In that context, "cyber operations may include reconnaissance (e.g., mapping a network), the seizure of supporting positions (e.g., securing access to key network systems or nodes), or the pre-placement of capabilities or weapons (e.g., implanting cyber access tools or malicious code)."[34] The US DOD also considers "cyber operations" to include a "method of acquiring foreign intelligence unrelated to specific military objectives, such as understanding [a] method of acquiring technological developments or gaining information about an adversary's military capabilities and intent."[35]

It is important to note that the US DOD's approach does not consider "activities that merely use computers or cyberspace without a primary purpose of achieving objectives or effects in or through cyberspace."[36] This includes "operations that use computer networks to facilitate command and control, operations that use air traffic

29. INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS, REPORT 31IC/11/5.1.2 36 (2011).
30. *Id.*
31. LAW OF WAR MANUAL, *supra* note 28, at § 16.1.2.
32. *Id.* at § 16.1.2.1.
33. *Id.*
34. *Id.*
35. *Id.* at § 16.1.2.1.
36. *Id.* at § 16.1.2.2.

control systems, and operations to distribute information broadly using computers[.]"[37] Likewise, operations that "target an adversary's cyberspace capabilities, but that are not achieved in or through cyberspace, would not be considered cyber operations." Therefore, "the bombardment of a network hub, or the jamming of wireless communications, would not be considered cyber operations, even though they may achieve military objectives in cyberspace."[38]

3. CYBER ATTACKS

The term "cyber attack," and by extension the term "cyberwar" are probably the most commonly misapplied terms in the rhetorical debate surrounding State cyber operations. For example, while the term "attack" has been used to describe the "defacement of websites, network intrusions, the theft of private information, or the disruption of the provision of internet services,"[39] it has legal significance within the *jus ad bellum*, triggering the right to exercise self-defense where there has been an "armed attack" within the meaning of Article 51 of the UN Charter and customary international law.[40] In other words, the phrase "cyber attack" is not "necessarily 'armed attacks' for the purpose of triggering a State's inherent right of self-defense under" the *jus ad bellum*.[41]

The term "cyberwar" is also subject to different interpretations. An early definition of cyberwarfare was "any operation that disrupts, denies, degrades, or destroys information resident in computers or computer networks."[42] Other scholars have described cyber operations, including web vandalism, disinformation campaigns and attacks on critical national infrastructure as "cyber war," using "war" as a "descriptive term and a rhetorical term, rather than a legal term."[43]

37. LAW OF WAR MANUAL, *supra* note 28, at § 16.2.2.
38. *Id.*
39. *Id.* at § 16.1.3.2.
40. *Id.*
41. *Id.*
42. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 132 (1999).
43. *See* Blank, *supra* note 3, at 79 (citing CTR. FOR THE STUDY OF TECH. & SOC'Y, SPECIAL FOCUS: CYBERWARFARE (2001)).

B. TYPES OF CYBER OPERATIONS

There are countless forms of cyber operations used by States and non-State actors. This article focuses on three: (1) DDoS attacks; (2) control system attacks; and (3) information gathering attacks.[44]

1. DDos Attacks

A DDoS attack is an "attempt to make a computer resource unavailable to its intended users, generally consisting of the concerted efforts of a person or people to prevent an internet site or service from functioning efficiently or at all."[45] DDoS attacks generally disrupt the availability of computer system resources to authorized users by sending data that causes the network to crash.[46] Stated another way, a DDoS attack:

> uses the power of hundreds or thousands of massed machines to impair the functioning of a particular website. Typically, an attacker will use a virus to take over control of a large number of computers that then form a botnet of 'zombie' machines. The attacker then programs the zombie computers to simultaneously log on to the targeted site. The exponential increase in traffic overwhelms the site's network, often requiring a temporary shutdown.[47]

The "botnets" are remotely controlled by one or more malicious actors, commonly referred to as "'botherders' or 'botmasters.'"[48] While having complete control over the bots:

> the botmaster is able to execute basically any action the legitimate owner of the computer could carry out, including instructing botnets to: (1) locate and infect other information systems with malware (which could allow botmasters to maintain and build their supply of new bots); (2) conduct distributed DDoS attacks; (3) rotate IP addresses under one or more domain names for the purpose of increasing the longevity of fraudulent websites; and (4) send spam, which can then distribute more

44. *See* Peter Margulies, *Soverignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELB. J. INT'L L. 496, 501 (2013); *see also* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 837, 839 (2012).

45. LIIS VIHUL ET AL., LEGAL IMPLICATIONS OF COUNTERING BOTNETS 4, n. 13 (2012).

46. *Id.*

47. Margulies, *supra* note 44, at 501.

48. *See generally* VIHUL ET AL., *supra* note 45, at 4.

malware.[49] In most cases, the goal of the DDoS is a financial gain.[50]

Stated another way, DDoS attacks are considered "flood attacks," and do not "normally penetrate into a computer system but aim to inundate the target with excessive calls, messages, inquiries, or requests in order to overload it and force it shut down.[51]

Over the past ten years there have been a number of well-known (and not so well-known) DDoS attacks launched against States where the perpetrator was suspected as being a State actor. In 2007, for example, Estonia was hit with a wave of DDoS attacks after it decided to remove a Soviet Bronze Soldier monument from its location in central Tallinn, Estonia to a military cemetery.[52] Ethnic Russians in Estonia had historically used the statue as a rallying site for demonstrations against the Estonian government,[53] and the removal of the statue sparked outrage from the Russian government, violence against the Estonian Ambassador in Moscow, indirect economic sanctions, and rioting amongst Estonia's ethnic Russian population. Over the next three weeks, Estonian government agencies, schools, banks and media outlets were hit with a series of DDoS attacks.[54] Estonian political parties also had their websites defaced with political messages.[55] The incident quickly drew worldwide attention, and the media labeled it the first "Cyber War."[56] All signs of the attack pointed to Russia. The "hackers claimed to be Russian, the tools to hack and deface were contained in Russian websites and chatrooms, and the attacks picked on May 9 (the day

49. *Id.*
50. *Id.*
51. Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 216 (Jens David Ohlin et al. eds., 2015) [hereinafter Roscini, *Evidentiary Issues*].
52. *See* Ian Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, THE GUARDIAN, May 16, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.
53. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED, Aug. 21, 2007, http://www.wired.com/2007/08/ff-estonia/.
54. Jason Richards, *Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security*, INT'L AFF. REV., http://www.iar-gwu.org/node/65 (last visited Aug. 15, 2016).
55. *Id*.
56. *Id*.

Russia celebrates Victory Day in Europe in World War II)."[57] And although the botnets included computers from different countries, at least some of the attacks "originated from Russian IP (internet protocol) addresses, including those of state institutions."[58] The timing of the attacks also implicated Russia, and Russia denied a request for bilateral investigation under the Mutual Legal Assistance Treaty between the two countries.[59] Russia is suspected to be the culprit of these attacks, but has taken no responsibility.

In 2008, Russia was suspected of carrying out another DDoS attack during its 2008 conflict with Georgia, which arose out of the 1992 South Ossetian War and the 1993 Abkhazian War.[60] "Three weeks before the war began, online attackers started assaulting Georgia's websites."[61] The attack involved fifty-four "web sites in Georgia related to communications, finance, and the government."[62] The attacks started "immediately before and continued throughout the armed conflict between the Caucasian state and the Russian Federation[.]"[63] All signs pointed to a Russian hacker community as the responsible perpetrator.[64] Coordination for the attacks took place in the Russian language, and in Russian or Russia-related "fora."[65] Like the Estonian attack, the level of sophistication and coordination of the attacks suggested governmental support for the attacks.[66] The DDoS attacks in Georgia represented the first time a State actor, or

57. Roscini, *Evidentiary Issues*, *supra* note 51, at 216 (citing WILLIAM A. OWENS ET AL., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 173 (2009)).

58. *Id.*

59. *Id.* (citing Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 208 (2009); ALEXANDER KLIMBURG, MOBILISING CYBER POWER 53 (2011).

60. David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS J., Jan. 6, 2011, at 1.

61. *Id.* at 2.

62. *Id.* (noting that many believed the attacks were carried out by "rogue elements within Russia"); *see* Jon Oltsik, *Russian Cyber Attack on Georgia: Lessons Learned?*, NETWORK WORLD (Aug. 17, 2009, 1:05 PM), http://www.networkworld.com/article/2236816/cisco-subnet/russian-cyber-attack-on-georgia—-lessons-learned-.html.

63. Roscini, *Evidentiary Issues*, *supra* note 51, at 216.

64. *Id.* (citing ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS. LEGAL CONSIDERATIONS 75 (2010).

65. *Id.*

66. *Id.*

forces tied to a State actor, used cyber operations to "prep the battlefield" for a kinetic attack.

Other examples include in 2010, the "Pakistani Cyber Army" shut down the website of India's top policy agency, the Central Bureau of Investigation, and defaced its systems.[67] And by 2013, a group named the "DarkSeoul Gang," a group suspected with ties to the North Korean State, was deemed responsible for at least four years of high-profile attacks in South Korea, including a DDoS attack and malicious code that wiped hard drives at South Korean banks, media and financial service companies, overwriting legitimate data with political messages.[68]

In 2014, Sony Pictures was hit with a highly publicized DDoS attack of unknown proportions after its computer systems were compromised by suspected North Korean tied hackers.[69] The attack surrounded the release of the movie "The Interview" about the fictional assassination of the North Korean leader, Kim Jong-un.[70] Prior to the movie's release, the spokesperson for North Korea's Ministry of Foreign Affairs said in a statement "that the country would take 'a decisive and merciless countermeasure' if the United States government permitted Sony to make its planned Christmas release of the comedy."[71] Although North Korea did not take credit for the ultimate attack, US officials traced the attack back to North Korea using the US's own cyber operations in North Korea.[72] In response, the US imposed economic sanctions on North Korea, and

67. *India and Pakistan in cyber war*, AL-JAZEERA, Dec. 4, 2010, http://www.aljazeera.com/news/asia/2010/12/20101241373583977.html.

68. Symantec Security Response, *Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War*, SYMANTEC, June 26, 2013, http://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war.

69. Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm*, N.Y. TIMES, Dec. 30, 2014, http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html (asserting that Sony was slow to realize the magnitude of the public relations complexities, financial loss, and uniqueness of the cyber attack).

70. THE INTERVIEW (Columbia Pictures 2014).

71. *See* Cieply & Barnes, *supra* note 69.

72. *See id*. (discovering that the party responsible was a hacking gang known as Dark Seoul).

North Korea suffered widespread Internet outages.[73]

2. Control System Attacks (Syntactic and Semantic Attacks)

Contrary to DDoS attacks, which impact access, control system attacks seek to compromise operating systems and alter data. There are generally two types of control system attacks: syntactic and semantic attacks. "Syntactic attacks use malicious computer code or malware such as 'worms', 'viruses', [and] 'Trojan horses' to compromise computer operating systems."[74] "Semantic attacks, [on the other hand], do not destroy the computer's operating system. [They] instead operate more subtly, and change the data generated by monitoring software while maintaining the illusion that the network is fully functional."[75] Semantic attacks are particularly harmful because they:

> aim to undermine control systems, such as the supervisory control and data acquisition (SCDA) system that regulates many of the machine's moving parts. SCADA systems govern the tolerances of machines such as turbines and centrifuges. Those systems can run at peak level for a limited period of time, after which they develop excess heat and begin to break down. Through semantic attacks, an attacker can alter the data recorded and displayed in SCADA systems. A machine running at peak capacity and approaching the limit of its tolerance can appear to be running at a far slower speed and temperature. Because the machine's operator does not see the correct data, the machine continues running when it should have been stopped and eventually self-destructs.[76]

Perhaps the most famous (or infamous) example of a semantic attack was Stuxnet. In January 2010, representatives of the International Atomic Energy Agency were visiting the Natanz uranium enrichment plant in Iran when they noticed "centrifuges used to enrich uranium gas were failing at an unprecedented rate."[77] Five months later, a computer security firm in Belarus was called to

73. *Id.*

74. Margulies, *supra* note 44, at 502; Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL L. REV 132, 139 (2005).

75. Margulies, *supra* note 44, at 502.

76. *Id.*

77. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's Largest First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

troubleshoot a series of computers in Iran that were crashing and rebooting repeatedly. The cause of the crash was a mystery until the firm found a handful of malicious files on one of the systems.[78] The files related to a computer worm dubbed "Stuxnet," which targeted the computer systems of five facilities located in Iran between June 2009 and May 2010.[79] The worm impacted industrial control systems which used a type of software developed by the Siemens company.[80] The attack resulted in centrifuges speeding up to an improper speed, effectively destroying themselves. The complexity of the attack led many to suspect the United States or Israel as the culprits.

In June 2012, the New York Times reported that the Stuxnet project, code-named "Operation Olympic Games," began during the George W. Bush administration and accelerated under President Obama.[81] The report also indicated that Stuxnet had been created with Israel's support, and was intended to contain a "weaponized" payload "designed to give instructions to other programs[.]"[82] Stuxnet represented the first known use of malicious code to result in material damage by attacking the SCADA system of national infrastructure.[83]

In February 2016, the New York Times also revealed that in the early years of the Obama administration, the United States developed a follow-up to Stuxnet named "Nitro Zeus," a carefully arranged plan to cyber attack Iran if efforts to limit to restrict its nuclear program failed.[84] The plan was devised to disable "Iran's air defenses, communications systems and crucial parts of its power grid, and was shelved, at least for the foreseeable future, after the nuclear deal struck between Iran and six other nations last summer was

78. *Id*.

79. KATHARINA ZIOLKOWSKI, STUXNET - LEGAL CONSIDERATIONS 3 (2012).

80. *Id.* (pointing out that the software configuration requirements were specific).

81. David P. Fidler, *Recent Developments and Revlations Concerning Cybersecurity and Cyberspace: Implications for International Law*, AM. SOC'Y INT'L L. INSIGHTS (June 20, 2012), https://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and.

82. Roscini, *Evidentiary Issues*, *supra* note 51, at 217.

83. *Id.* (citing Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD., 1, 7-20 (2012)).

84. Sanger & Mazzetti, *supra* note 13.

fulfilled."[85] At its height, officials say the planning for Nitro Zeus involved "thousands of American military and intelligence personnel, spending tens of millions of dollars and placing electronic implants in Iranian computer networks to 'prepare the battlefield,' in the parlance of the Pentagon."[86] While the Pentagon was making those preparations, American intelligence agencies were developing an operation that "would have inserted a computer 'worm' into the facility with the aim of frying Fordo's computer systems—effectively delaying or destroying the ability of Iranian centrifuges to enrich uranium at the site. 'Nitro Zeus' was intended as a follow-up to 'Olympic Games'" (i.e., Stuxnet).[87]

4. Information Gathering/Data Destruction Attacks

Perhaps the most commonly used cyber operation by States (or non-State actors acting at the behest of State actors) over the past ten years has been information gathering attacks. These attacks essentially steal information and gather data. Some notable examples include:

- In 2009 Canadian researchers discovered that hackers tied to the Chinese State controlled a global cyber espionage network in over 100 countries.[88]
- In 2010, a Chinese telecommunications firm transmitted false routing information for 37,000 computer networks, misrouting internet traffic through China and exposing data from 8,000 US networks, 1,100 Australian networks, and 230 French networks.[89]
- In 2010, suspected hackers tied to the Chinese State stole the blueprints for the Australian Security Intelligence Organization's new $631 million building scheduled for completion in 2013.[90]

85. *Id.* (noting that such preparation indicated President Obama's belief that the nuclear talks could fail, and that subsequent drastic matters would need to be taken).

86. *Id.*

87. *Id*.

88. *See* INFO. WARFARE MONITOR, TRACKING GHOSTNET: INVESTIGATING A CYBER ESPIONAGE NETWORK 5 (2009).

89. See Jaikumar Vijayan, *Update: Report sounds alarm on China's rerouting of U.S. Internet traffic*, COMPUTERWORLD, Nov. 18, 2010, http://www.computerworld.com/article/2514493/network-security/update—report-sounds-alarm-on-china-s-rerouting-of-u-s—internet-traffic.html.

90. Assoc. Press, *Report: Plans for Australia spy HQ hacked by China*, May

- In 2010, Google reported that the gmail user accounts of Chinese human rights activists were accessed, as well as the email accounts of 30 other California companies.[91] The Chinese State is largely suspected as the culprit.
- In 2011, hackers suspected with ties to the Iranian State compromised a Dutch digital certificate authority, issuing more than 500 fraudulent corporate certificates for major companies and government agencies.[92]
- In 2012, a hacker group tied to the Iranian State called the "Cutting Sword of Justice" used the "Shamoon" virus to attack the Saudi Arabian national oil company Aramco, deleting data on three-quarters of Aramco's corporate PCs, including documents, spreadsheets, e-mails, and files, and replacing them with an image of a burning American flag.[93]
- In 2013, the Syrian Electronic Army hacked three widely used communications platforms: (1) Tango; (2) Viber; and (3) Truecaller. The attack exposed the communications of millions of people to the Syrian intelligence services, including the communications of political activists.[94]
- In 2015, cyber operations hit the U.S. Office of Personnel Management, and a total of 22.1 million people, mainly federal workers, had their personal data stolen. The information stolen included sensitive data information such as Social Security numbers, fingerprints, passwords, and information used in conducting background screening for security clearances.[95] According to a report by the U.S. Department of Homeland Security (DHS), there were nine major cyber attacks aimed at millions of Americans' personal data through federal and private

28, 2013.

91. Malcolm Moore, *Chinese human rights activists claim their Google emails were hacked*, TELEGRAPH, Jan. 15, 2010, http://www.telegraph.co.uk/news/worldnews/asia/china/6996906/Chinese-human-rights-activists-claim-their-Google-emails-were-hacked.html.

92. Robert Charette, *DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands*, IEEE SPECTRUM, Sept. 9, 2011, http://spectrum.ieee.org/riskfactor/telecom/security/diginotar-certificate-authority-breach-crashes-egovernment-in-the-netherlands.

93. Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S Sees Iran Firing Back*, N.Y. TIMES, Oct. 23, 2012, http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html.

94. Anupika, Khare, *Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts*, IDIGITAL TIMES, July 19, 2013.

95. Keith Wagstaff & Matthew DeLuca, *21.5 Million Affected by Massive Background Check Breach*, MSNBC (July 9, 2015, 3:51 PM), http://www.msnbc.com/msnbc/opm-215-million-affected-massive-background-check-breach.

computer networks.[96]

- A recent review of federal records obtained by *USA Today* revealed that, between 2010 and 2014, the U.S. Department of Energy (DOE) was hit with 159 successful cyber intrusions,[97] showing a "near-consistent barrage of attempts to breach the security of critical information systems that contain sensitive data about the nation's power grid, nuclear weapons stockpile and energy labs."[98] The records showed that DOE components reported "a total of 1,131 cyberattacks over a forty-eight month period ending in October 2014."[99] Of those attempted cyber intrusions, 159 were successful.[100] The same records indicated that the "National Nuclear Security Administration, a semi-autonomous agency within the Energy Department responsible for managing and securing the nation's nuclear weapons stockpile, experienced nineteen successful attacks during that same period."[101]

C. THE *JUS AD BELLUM* EXPLAINED

To understand how international norms apply to these State directed or approved cyber operations, it is first important to understand the basic principles of public international law, and, relevant to this article, the norms constituting the *jus ad bellum*.

1. International Law - General Principles

Public international law is the body of law that regulates State conduct. There are two accepted "hard sources" of public international law: (1) treaties and (2) custom. Generally, if State action is not expressly prohibited by either a treaty or a customary norm, it is permitted.[102] That is so because public international law is

96. Bill Gertz, *OPM Hack Part of Large-Scale Cyber Attack on Personal Data*, WASH. FREE BEACON, July 16, 2015, http://freebeacon.com/national-security/opm-hack-part-of-large-scale-cyber-attack-on-personal-data/ (citing a Department of Homeland Security report covering the summer of 2014 to July of 2015).

97. Steve Reilly, *Records: Energy Department Struck by Cyber Attacks*, USA TODAY, Sept. 11, 2015, http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/.

98. *Id.*

99. *Id.*

100. *Id.*

101. *Id.* (adding that the specific nature of the attacks was redacted from the records before being released).

102. *See* S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, ¶¶

premised upon the bedrock principle of State sovereignty, and the concept of State consent.[103]

In addition to the two "hard sources" of public international law, there are also recognized "soft sources" used as a subsidiary means for the interpretation and application of treaties and custom. Most notably, the Statute of the International Court of Justice (ICJ), the official judicial organ of the UN, lists "general principles of law" and the "judicial teachings of the most highly qualified publicists of the various nations" as "subsidiary means for the determination of the rules of law."[104] It is unsettled whether the order of norms and sources in Article 38 of the ICJ Statute represent a hierarchy of norms.[105]

a. Treaties - Basic Principles

The word treaty is a "generic term embracing all instruments binding under international law, regardless of their formal designation, concluded between two or more international juridical persons."[106] Treaties may be concluded between: (a) States; (b) international organizations with treaty-making capacity and States; or (c) international organizations with treaty-making capacity.[107] The application of the term treaty signifies that the parties "intend to create rights and obligations enforceable under international law."[108] The 1969 Vienna Convention on the Law of Treaties ("VCTL") defines a treaty as "an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related

53, 96 (Sept. 7) (finding no prohibition existed in international law against a state prosecuting a foreign seaman for a collision on the high seas, and therefore the prosecution was permissible).

103. Schmitt, *Cyber Warfare*, *supra* note 21, at 272-73.

104. Statute of the International Court of Justice, U.N. Charter, annex, art. 38; *see also* Michael N. Schmitt & Liis Vihul, *The Nature of International Law Cyber Norms*, TALLINN PAPERS, no. 5, 2014, at 1, 3.

105. *See* PIERRE-MARIE DUPUY, DROIT INTERNATIONAL PUBLIC 14-16 (1992) (arguing that there is no hierarchy in international law norms, and there can be none).

106. TREATY SECTION OF THE OFFICE OF LEGAL AFFAIRS, UNITED NATIONS, TREATY HANDBOOK 64 (2006).

107. *Id.*

108. *Id.*

instruments and whatever its particular designation."[109]

There are no treaties governing the cyber relations between States generally. Instead, customary international law is largely the international normative space one must look to understand the principles governing and restricting State directed or approved cyber operations.

b. Customary International Law - Basic Principles

Customary international law is generally defined as the "collection of international behavioral regularities that nations over time come to view as binding as a matter of law."[110] Stated differently, customary international law is the general practice of States accepted as law.[111]

For a practice to reach the level of a customary norm, two elements must be satisfied. First, the practice must have long-term, widespread compliance by States.[112] Evidence of State practice must be "both extensive and representative."[113] It does not, however, need to be universal in the broad sense of the term.[114] No "precise number or percentage is required because it is not simply a question of how many states participate in the practice, but also which states participate."[115] And whether certain State practice has achieved the long-term, widespread compliance necessary for normative effect is a question of fact.[116] Both physical and verbal acts of States may

109. Vienna Convention on the Law of Treaties art. 2(1)(a), May 23, 1969 1155 U.N.T.S. 331.

110. Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law* 5 (Univ. Chi. Law Sch., John M. Olin Law & Economics Working Paper No. 63 (2d Series), 1999).

111. Statute of the International Court of Justice, art. 38(1)(b).

112. Lynn Loschin, *The Persistent Objector and Customary Human Rights Law: A Proposed Analytical Framework*, 2 U.C. DAVIS J. INT'L L. & POL'Y 147, 148 (1996) (explaining that state compliance is established through duration, uniformity, consistency, and generality of the practice).

113. *Id.*

114. *See* INT'L LAW ASS'N, STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW 23 (2000); Jean-Marie Henckaerts, *Assessing the Laws and Customs of War: The Publication of Customary International Humanitarian Law*, 13 HUM. RTS. BRIEF 8, 9 (2006).

115. Henckaerts, *supra* note 114, at 8; INT'L LAW ASS'N, STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW ¶¶ 14(d)-(e) (2000).

116. *See* Henckaerts, *supra* note 114, at 8-9 (pointing to official state reports, domestic legislation and case law, and diplomatic statements as sources for

constitute practice that contributes to the creation of customary international law.[117] Resolutions adopted by States in international organizations or at conferences may also have a normative effect, depending on their "content, degree of acceptance, and the consistency of related practice."[118]

There is no specified time frame in which a rule of customary international law must emerge. Instead, "[S]tate practice has to be weighed to assess whether it is sufficiently 'dense' to create a rule of customary international law, which means that it has to be virtually uniform, extensive, and representative."[119] To be virtually uniform, State practice must mean that "different [S]tates have not engaged in substantially different conduct."[120] However, contrary practice that appears to undermine the uniformity of the practice does not necessarily prevent the formation of a customary international legal principle if the contrary practice is condemned by other States.[121]

Second, States must believe conformance with the purported widespread practice is mandatory.[122] This second element is

evidence of state practice).

117. *See id.* at n. 6 (noting that physical acts include battlefield behavior, the use of certain weapons, and the treatment afforded to different categories of persons. Verbal acts include military manuals, national legislation, national case-law, instructions to armed and security forces, military communiques during war, diplomatic protests, opinions of official legal advisers, comments by governments on draft treaties, executive decisions and regulations, pleadings before international tribunals, statements in international fora, and government positions on resolutions adopted by international organizations).

118. Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 70 (July 8); Henckaerts, *supra* note 114, at 9.

119. Sir Humphrey Waldock, *General Course on Public International Law*, 106 COLLECTED COURSES HAGUE ACAD. INT'L L. 44 (1962) (discussing the elements of international law, specifically density, which depends on the nature of the case); *see also* Henckaerts, *supra* note 114, at 9.

120. Henckaerts, *supra* note 114, at 9 (stating that customary international law should be "virtually uniform[,]" which means that state actions should not be "substantially different" from one another).

121. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 186 (June 27); *see also* Henckaerts, *supra* note 114, at 9.

122. *See* North Sea Continental Shelf (Ger./Den.; Ger./Neth.), Judgment, 1969 I.C.J. 3, ¶ 77 (Feb. 20) (stressing that a state's compliance with a practice alone, no matter how consistently, would not suffice to constitute customary international law without evidence that the practice was rendered obligatory by the existence of a rule of law requiring it).

commonly referred to as the *opinio juris*. Once a practice satisfies these two elements it is considered binding upon all States, except those that "persistently object" during the normative development.[123] The requirement of *opinio juris* in establishing the existence of customary international law refers to the legal conviction that a particular practice is carried out as if it were required by law.[124] It is usually not necessary to demonstrate separately the existence of an *opinio juris* because it is generally contained within a particular dense practice. Where situations are ambiguous, however, *opinio juris* plays an important role in figuring out whether or not state practice counts toward the formation of customary international law. If a State wants to change an existing rule of customary international law, it must do so through official practice and claim the requisite *opinio juris*.[125]

2. Jus Ad Bellum *Principles*

The *jus ad bellum* is a subset of public international law governing when, and in what manner, States may use force vis-à-vis one another. The *jus ad bellum* is rooted in the fundamental principles of State sovereignty and non-intervention, which prohibits the use of force generally with certain exceptions.

a. Sovereignty

The concept of State sovereignty is the bedrock of modern international law. Rooted in the Treaty of Westphalia, State sovereignty ensures States respect, and honor the physical and legal boundaries established through centuries of practice.

The most widely accepted definition of State sovereignty comes from the *Island of Palmas* Arbitral Award of 1928, which states that

123. *See id.* at ¶ 37 (holding that customary international law is equally binding on all members of the international community); Loschin, *supra* note 112, at 148 (stating that the use of reservations has undercut the goal of creating truly universal law).

124. *North Sea Continental Shelf*, 1969 I.C.J. at 3, ¶ 77 (stressing the importance in a state's belief that a practice is obligatory); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 8 (7th ed. 2008) (arguing *opinio juris* is a necessary ingredient in determining customary law); LORI F. DAMROSCH ET AL., INTERNATIONAL LAW: CASES AND MATERIALS (4th ed. 2001).

125. *See* DAMROSCH ET AL., *supra* note 124.

sovereignty "in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[126] Sovereignty therefore includes the right of a State to "control access to its territory" and generally enjoy "within the limits set by treaty and customary international law, the exclusive right to exercise jurisdiction and authority on its territory."[127]

b. Non-Intervention

A corollary principle to State sovereignty is the principle of non-intervention. Non-intervention is a general principle of customary international law,[128] involving the right of "every sovereign State to conduct its affairs without outside interference."[129] Although the "precise scope and content of the non-intervention principle remains the subject of some debate,"[130] it is widely accepted as customary international law.

But not all outside, State interference automatically constitutes unlawful intervention in violation of the principle of non-intervention. "Interference pure and simple is not intervention."[131] Instead, customary international law recognizes two types of State practice that run afoul of the principle of non-intervention: (1) the use or threat of "force" and (2) the use of non-forceful but coercive intervention.

126. Island of Palmas (Neth./U.S.), 2 R.I.A.A. 829, 838 Hague Ct. Rep. 2d (Scott) 829, 838 (Perm. Ct. Arb. 1928).

127. TALLINN MANUAL, *supra* note 17, at 16 (implying that states enjoy the right to control whatever falls within its territory).

128. U.N. Charter art. 2, ¶ 4; Armed Activities on Territory of Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶¶ 163-65 (Dec. 19) (noting violation of the general principle); Legal Consequences of Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 87 (July 9) (citing U.N. Charter); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27); G.A. Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, at 123 (Oct. 24, 1970).

129. *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 202.

130. TALLINN MANUAL, *supra* note 17, at 44, ¶ 7.

131. 1 OPPENHEIM'S INTERNATIONAL LAW: PEACE 432 (Robert Jennings & Arthur Watts eds., 9th ed. 1992) (emphasizing that intervention must be forcible or dictatorial).

Moreover, the principle of non-intervention is not absolute. There are three (perhaps four) recognized exceptions: (1) invitation; (2) Security Council authorization, and (3) collective and individual self-defense exercised pursuant to Article 51 of the UN Charter. The fourth, some have argued, is the Responsibility to Protect ("RtoP") doctrine, an arguably emerging doctrine that would make previously unlawful humanitarian intervention lawful under the theory that States exercising "responsibility" (as opposed to "intervening") in foreign States to protect those in need would not run afoul of the principle of non-intervention.

3. Prohibition Against the Use or Threat of Force

The prohibition against the use or threat of force is embodied in Article 2(4) of the UN Charter, which provides:

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.[132]

This general principle is reflective of customary international law, as it is embodied within General Assembly resolution 2625 (XXV), entitled "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations," which has been recognized as reflecting customary international law.[133] Along these lines, a number of other instruments, including the Charter for the Organization of American States[134] and the Final Act of the Helsinki Conference on Security and Co-operation in Europe of 1 August, 1975 reaffirm the principle of non-intervention and the prohibition against the use of "force."[135]

132. U.N. Charter art. 2, ¶ 4.

133. *Nicar. v. U.S.*, 1986 I.C.J. at ¶¶ 191-93, at 101-03; G.A. Res. 2625 (XXV), *supra* note 128, at 122.

134. Charter of the Organization of American States art. 19, Apr. 30, 1948 [hereinafter OAS Charter].

135. *Id.*; Organization for Security and Co-operation in Europe [OSCE], *Conference on Security and Co-operation in Europe Final Act*, at art. 5, (Aug. 1, 1975).

What constitutes "force," and what amounts to either a "use" or "threat of force" has been the subject of extensive debate. For example, although there is no "authoritative definition of, or criteria for, 'threat' or 'use of force'," [136] we do know that certain categories of coercive operations do not amount to a use of "force," such as economic coercion.[137]

We also know that a use of force may not necessarily involve employment of military or armed forces by the State in question. In the ICJ's *Nicaragua* opinion, for example, the ICJ found that arming and training a guerrilla force that is engaged in hostilities against another State qualified as a use of force.[138] This tracks the ICJ's later advisory opinion on the use of nuclear weapons, which stated that the prohibition of the use of force applies to "any use of force, regardless of the weapons employed."[139]

The "threat" component of Article 2(4) gone largely unstudied. The ICJ framed the concept:

> Whether a signaled intention to use force if certain events occur is or is not a 'threat' within Article 2, paragraph 4, of the Charter depends upon various factors. If the envisaged use of force is itself unlawful, the stated readiness to use it would be a threat prohibited under Article 2, paragraph 4. Thus it would be illegal for a State to threaten force to secure territory from another State, or to cause it to follow or not follow certain political or economic paths. The nations of 'threat' and 'use' of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal—for whatever reason—the threat to use such force will likewise be illegal. In short, if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter. For the rest, no State—whether or not it defended the policy or deterrence—suggested to the Court that it would be lawful to threaten to use force if the use of force contemplated would

136. TALLINN MANUAL, *supra* note 17, at 46.

137. The concept of economic coercion constituting "force" within the meaning of Article 2(4) of the UN Charter was rejected during the 1945 UN Charter drafting conference in San Francisco. 6 U.N.C.I.O. Docs. 334, 609 (1945); Doc. 2, 617(e)(4), 3 U.N.C.I.O. Docs 251, 253-54 (1945). Economic coercion could still nonetheless violate the principle of non-intervention as discussed herein.

138. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 228 (June 27).

139. Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

be illegal.[140]

4. Unlawful Interference Less Than Force

Interference that does not rise to the level of a threat or use of force may nonetheless violate the principle of non-intervention if it is intended to coerce the political, economic, social or cultural system of another State.[141] In *Nicaragua*, for example, the ICJ stated that the "principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference[.]"[142] This includes intervention "directly or indirectly in the internal or external affairs of other States," including intervention into a State's choice of a "political, economic, social and cultural system, and the formulation of foreign policy."[143] According to the ICJ, intervention is wrongful "when it uses methods of coercion in regard to such choices, which must remain free ones"[144] and that a "prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely."

The Charter for the Organization of American States recognizes a similar distinction, stating at Article 19 that no State or group of States:

> has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. The foregoing principle prohibits not only armed force but also any other form of interference or attempted threat against the personality of the State or against its political, economic, and cultural elements.[145]

5. Recognized Exceptions

There are three well recognized exceptions and one controversial exception to the principle of non-intervention: (1) State consent; (2) UN Security Council authorization; (3) collective and individual self-

140. *Id.* at ¶ 47.
141. OAS Charter, *supra* note 134, at art. 19; *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 205.
142. *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 202.
143. *Id.* at ¶ 205.
144. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 205 (June 27).
145. OAS Charter, *supra* note 134, at art. 19.

defense; and, arguably, (4) the RtoP doctrine. These exceptions are discussed in detail below.

a. State Consent

Intervention, including military intervention, is not prohibited if it is conducted in accordance with the consent of the intervened upon State. In a study of State responsibility for wrongful conduct, the International Law Commission concluded that consent to intervention acts as a form of bilateral agreement between the consenting and intervening States that suspends the normal operation of the legal rules that would otherwise govern their relationship.[146] In many cases, consent is "often a highly controversial justification for military intervention."[147]

b. UN Security Council Authorization

Article 39 of the UN Charter makes clear that the Security Council has the sole authority within the UN framework to "determine the existence of a threat to the peace, breach of the peace, or act of aggression," and "shall" make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42 of the Charter to "maintain or restore international peace and security."[148] Article 41 authorizes the Security Council to take measures "not involving the use of armed force" to "give effect to its decisions," including "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[149] Article 42 authorizes the Security Council to authorize "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security" if those measures authorized by Article 41 are "inadequate or have proved to be inadequate[.]"[150] Such action may include "demonstrations, blockade, and other

146. David Wippman, *Military Intervention, Regional Organizations, and Host-State Consent*, 7 DUKE J. COMP. & INT'L L. 209, 210 (1996) (citing Eight Report on State Responsbility, Document A/CN.4/318 and Add.1-4, 2 Y.B. INT'L COMM'N 3, 35-36 (1979)).

147. *Id.* at 209.

148. U.N. Charter art. 39.

149. U.N. Charter art. 41.

150. U.N. Charter art. 42.

operations by air, sea, or land forces of Members of the United Nations."[151]

c. Collective and Individual Self-Defense

Article 51 of the UN Charter provides as follows:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[152]

Only force that is of sufficient gravity will constitute an "armed attack" within the meaning of Article 51.[153] And although there have been debates about the right to engage in "anticipatory self-defense" within the framework of Article 51, most governments and scholars, including the ICJ, appear to agree that self-defense is permitted under Article 51 of the UN Charter only when there has been an "armed attack" by another State.[154]

In the case of non-State actors, the ICJ in *Nicaragua* stated that an "armed attack" would occur when regular armed forces cross an international border, or when a state sends "armed bands, groups, irregulars or mercenaries which carry out acts of armed force against another State of such gravity as to amount" to an actual armed attack by regular forces.[155] An "armed attack" must therefore have a "trans-border element."[156] Therefore, determining whether a particular "attack" rises to the level of an "armed attack" is critical, as it may

151. *Id.*

152. U.N. Charter art. 51.

153. *See* Sean D. Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 HARV. INT'L L. J. 41, 44 (2002).

154. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 103 (June 27); Murphy, *supra* note 153, at 44.

155. *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 103 (stating the exercise of self-defense in the international arena as a right is subject to whether the State was a victim of an armed attack).

156. TALLINN MANUAL, *supra* note 17, at 54.

trigger the right to individual or collective self-defense under Article 51 of the UN Charter.

d. RtoP Doctrine

The RtoP doctrine is an attempt to create a fourth "exception" to the principle of non-intervention. But, it's not actually an "exception" *per se*. The RtoP doctrine, if adopted as law, imposes a duty on States to protect their own citizens from certain war crimes, crimes against humanity and genocide. This duty is seen as a corollary obligation to the duties incumbent upon sovereign States, which include the hallmark requirements that a State have territory and exercise governmental functions. This responsibility to protect carries with it significant consequences if it is not followed. According to the RtoP doctrine, any failure to carry out the duty to protect would transfer said obligation to the international community as a whole, thereby authorizing an "intervention" into that State's sovereign space without violating the principle of non-intervention. As some scholars have noted, this new "formulation (a duty on the part of [S]tates to protect civilians) sounds significantly better than an *exception to a prohibition* on interfering with another State's territory."[157] Otherwise, without the RtoP doctrine, and without UN Security Council authorization, intervention for humanitarian purposes "implies a contravention of the traditional norms of sovereignty and non-intervention, principles that have been at the heart of the international legal structure."[158]

Whether the RtoP doctrine has risen to the level of customary international law is subject to extensive debate. The development of the doctrine was born out of the unchecked atrocities in Rwanda, and the confusing legal justifications surrounding NATO's intervention Kosovo in 1999. In 2000, then former UN Secretary-General Kofi Anan asked the UN General Assembly, "If humanitarian intervention is, indeed, an unacceptable assault on sovereignty, how should we respond to a Rwanda, to a Srebrenica—to gross and systematic

157. Sara Dillon, *Yes, No, Maybe: Why No Clear "Right" Of The Ultra-Vulnerable To Protection Via Humanitarian Intervention?*, 20 MICH. ST. INT'L L. REV. 170, 190 (2012).

158. Peter Stockburger, *The Responsibility to Protect Doctrine: Customary International Law, an Emerging Norm, or Just Wishful Thinking?*, 5 INTERCULTURAL HUM. RTS. L. REV. 365, 396 (2010).

violations of human rights?"[159] In 2000, in response to this challenge, the Government of Canada, together with a group of major foundations, announced at the UN General Assembly the establishment of the International Commission on Intervention and State Sovereignty ("ICISS").[160] In November 2001, ICISS issued its report entitled "The Responsibility to Protect," which produced a framework for the R2P doctrine.

The endorsement of the ICISS report came fairly quickly. In December 2004, the ideas and principles of the ICISS report were officially endorsed by the Secretary-General's High-Level Panel on Threats, Challenges and Change in a 2004 report titled "A More Secure World: Our Shared Responsibility."[161] The Secretary-General then endorsed the RtoP report in his own 2005 report entitled "In Larger Freedom," which was adopted in the Outcome Document of the World Summit by the UN General Assembly in September 2005.[162] Shortly thereafter, regional organizations, such as the African Union, adopted similar principles.[163] Nearly one year after the 2005 World Summit, in a debate over authorization to send UN Peacekeepers to Darfur, Sudan, UN members "unanimously accepted the responsibility to protect populations from genocide, ethnic cleansing, war crimes and crimes against humanity, pledging to take action through the Security Council when national authorities fail."[164] The UN Security Council subsequently adopted Resolution 1674,

159. *Id.* at 373.

160. *See* INT'L COMM'N ON INTERVENTION AND ST. SOVEREIGNTY, THE RESPONSIBILITY TO PROTECT: REPORT OF THE INTERNATIONAL COMMISSION ON INTERVENTION AND STATE SOVEREIGNTY (Dec. 2001), at VII.

161. *See generally* Rep. of the High-Level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility*, ¶¶ 201-302, U.N. Doc. A/59/565 (Dec. 2, 2004) (deciding to endorse largely based on the successive humanitarian disasters, including those in Somalia, Bosnia and Herzegovina, Rwanda, Kosovo and Darfur).

162. U.N. Secretary-General, In Larger Freedom: Towards Development, Security and Human Rights for All, at 1, U.N. Doc. A/59/2005/Add.3 (May 26, 2005).

163. *See* Rep. of the African Union, *The Common African Position on the Proposed Reform of the United Nations: "The Ezulwini Consensus"*, at 1, 7 Ext/EX.CL/2 (VII) (Mar. 7-8, 2005) (emphasizing peacekeeping measures and post conflict peace-building steps).

164. Dana Michael Hollywood, *It Takes a Village . . . or at Least a Region: Rethinking Peace Operations in the Twenty-First Century, the Hope and Promise of African Regional Institutions*, 19 FLA. J. INT'L L. 75, 102 (2007).

reaffirming "the [provisions] . . . of the 2005 World Summit Outcome Document regarding the responsibility to protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity."[165]

This widespread endorsement of the R2P doctrine is notable. Rarely has an international principle received such widespread endorsement in such a rapid fashion. In 2008, during an address at an event on sovereignty in Berlin, Germany, UN Secretary-General Ban Ki-moon clarified his support for the RtoP doctrine.[166] That speech was followed by a 2009 Secretary-General report entitled "Implementing the responsibility to protect," which was presented to the 63rd session of the UN General Assembly.[167] During subsequent informative interactive dialogues and debates, scholars and state representatives expressed a variety of views on the doctrine. The European Union stated that it favors the adoption of the RtoP doctrine within the current framework of international law.[168] The Non-Aligned Movement, however, does not. The Non-Aligned Movement is a movement comprising of approximately 118 States and two-thirds of the UN's members.[169] The Non-Aligned Movement noted there are "concerns about the possible abuse of [RtoP] by expanding its application to situations that fall beyond the four areas defined in the 2005 World Summit Document, misusing it to legitimize unilateral coercive measures or intervention in the internal

165. S.C. Res. 1674, ¶ 4 (Apr. 28, 2006).

166. *See generally* Press Release, Secretary-General, Secretary-General Defends, Clarifies 'Responsibility to Protect' at Berlin Event on 'Responsible Sovereignty: International Cooperation for a Changed World,' U.N. Press Release SG/SM/11701 (July 15, 2008) (distinguishing the responsibility to protect from humanitarian intervention and human security).

167. U.N. Secretary-General, Implementing the Responsibility to Protect, at 1, U.N. Doc. A/63/677 (Jan. 12, 2009) (proposing strategies, tools, processes and practices to be implemented so states can be prepared to properly implement the responsibility to protect).

168. *See* Anders Lidén (Ambassador and Permanent Representative of Sweden to the United Nations), *Statement on Behalf of the European Union, General Assembly Debate on the Responsibility to Protect*, 63rd Sess., 97th Plenary Meeting (July 23, 2009) (suggesting the responsibility to protect should extend past simply stopping atrocities, into proactive developmental strategies to avoid atrocities).

169. *See generally* Cedric Grant, *Equity in International Relations: A Third World Perspective*, 71 INT'L AFF. 567, 568-70 (1995) (explaining the development and growth of NAM).

affairs of States."[170] In 2011, the US used the language of the RtoP doctrine to justify its air campaign in Libya. And many believe the RtoP doctrine could be, and should be used, in Syria.

6. State Responsibility and Attribution

Another critical area of international law that must be understood before applying international norms to cyberspace is the concept of State responsibility and attribution.

Generally, a State bears international legal responsibility for operations attributable to it and which constitute a breach of an international obligation. This is often referred to as the customary international law of State responsibility and is largely reflected in the International Law Commission's Articles on State Responsibility.[171] All acts or omissions of organs of a State are automatically and necessarily attributable to that State.[172] This concept is broad, and every person or entity that has that status under the State's internal legislation will be an organ of the State regardless of their function or place in the governmental hierarchy.[173]

With regard to non-State actors, Article 8 of the Articles on State Responsibility states that the conduct of a person or group of persons "shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[174] The ICJ has clarified this standard to mean that, at least within the context of military operations, a State is responsible for

170. Maged A. Abdelaziz (Permanent Representative of Egypt to the United Nations), *Statement on Behalf of the Non-Aligned Movement on Agenda Item 44 and 107: "Integrated and Coordinated Implementation of and Follow-up to the Outcomes of the Major United Nations Conferences and Summits in the Economic, Social and Related Fields; Follow-up to the Outcome of the Millennium Summit: Report of the Secretary-General*" (July 23, 2009) (encouraging that the responsibility to protect should be limited specifically to genocide, war crimes, ethnic cleansing and crimes against humanity).

171. U.N. International Law Commission, Report of the International Law Commission, Draft Articles of State Responsibility, U.N. GAOR, 53rd Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001).

172. G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts, art 4(1) (Dec. 12, 2001).

173. *See id.* art. 4(2) ("an organ includes any person or entity which has status").

174. G.A. Res. 56/83, *supra* note 172, art. 8.

the acts of non-State actors where it has "effective control" over such actors.[175] A competing standard was articulated by the International Criminal Court for the Former Yugoslavia (ICTY) which adopted an "overall control" test, which is a lower threshold inquiry.[176] Under the "overall control" test, the requisite control must go beyond "the mere financing and equipping of such forces and involv[e] also participation in the planning and supervision of military operations."[177]

III. THE TALLINN MANUAL CONCLUSIONS AND KNOWN UNKNOWNS

The authors of the TALLINN MANUAL examined these principles, and specifically whether, and to what extent, they apply to State directed or approved cyber operations. The IGE was "unanimous in its estimation" that the *jus ad bellum* applies to cyber operations,[178] and sought out to determine "how such laws applied, and to identify any cyber-unique aspects thereof."[179] The "Rules" in the TALLINN MANUAL therefore "reflect consensus among the" IGE "as to the applicable *lex lata*, that is, the law currently governing cyber conflict. It does not set forth *lex ferenda*, best practice, or preferred policy."[180]

In terms of how the IGE reached its conclusions, the TALLINN MANUAL provides:

175. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27) (establishing the "effective control" test and finding the United States' sharing of intelligence and financing with the contras did not satisfy the "effective control" test because the United States did not have inherent control over the contras); *but see* Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 43, ¶¶ 399-401 (Feb. 26) (altering the test for "effective control" to simply require an organ to act in accordance with a state's instructions and those actions result in the violations).

176. *See* Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶¶ 131, 145 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999), http://www.icty.org/case/tadic/4.

177. *Id.* at ¶ 145.

178. TALLINN MANUAL, *supra* note 17, at 5.

179. *Id.*

180. *Id.*

> When treaty law directly on point or sufficient State practice and *opinio juris* from which to discern precise customary international law norms was lacking, the International Group of Experts crafted the Rules broadly. In these cases, the Experts agreed that the relevant principle of law extended into the cyber realm, but were hesitant to draw conclusions as to its exact scope and application in that context. Where different positions as to scope and application existed, they are reflected in the accompanying Commentary. [¶] To the extent the Rules accurately articulate customary international law, they are binding on all States, subject to the possible existence of an exception for persistent objectors. [¶] The Rules were adopted employing the principle of consensus within the International Group of Experts. All participating experts agreed that, as formulated, the Rules replicate customary international, unless expressly noted otherwise. It must be acknowledged that at times members of the Group argued for a more restrictive or permissive standard than that eventually agreed upon. The Rule that emerged from these deliberations contains text regarding which it was possible to achieve consensus.[181]

Below is an examination of the TALLINN MANUAL's conclusions as they pertain to the concepts of State responsibility, use of force, armed attack and humanitarian intervention and an identification of the known unknowns that remain.

A. STATE RESPONSIBILITY

Attributing cyber operations to State actors is extremely difficult. In 2010, during a military exercise that simulated a sophisticated cyber attack it became apparent that no one "could pinpoint the country from which the attack came . . . ."[182] The difficulty in cyber attribution can also be seen in the 2007 and 2008 attacks in Estonia and Georgia. In each, Russia denied responsibility because there was no public evidence directly linking the Russian State to either attack.

On the flipside, the US was able to quickly attribute the 2014 Sony attack to the North Korean State. And the recent hacking of the Democratic National Committee has been attributed to the Russian State. So, attribution is possible. The critical question is what test of attribution under international law should apply to State sponsored or

181. *Id.* at 6.

182. John Markoff et al., *In Digital Combat, U.S. Finds No Easy Deterrent*, N.Y. TIMES, Jan. 26, 2010, http://www.nytimes.com/2010/01/26/world/26cyber.html.

directed cyber attacks?

The authors of the TALLINN MANUAL do not take a firm position as to whether the *Nicaragua* "effective control" test or the ICTY "overall control" test should apply to cyber operations, but the IGE does note that the "effective control" test is "particularly relevant" in the cyber context.[183] Until there is further state practice and jurisprudence from the ICJ, this remains a known unknown. The authors of the TALLINN MANUAL recognized that attribution in cyberspace remains an "ongoing challenge due to a series of complicating factors such as the ability of an unknown aggressor to mimic the tools, techniques, and procedures of a better-known aggressor with whom the target already has tense relations."[184]

In the cyber context, the authors of the TALLINN MANUAL proffered examples of such a scenario, including where "a private corporation that has been granted the authority by the government to conduct offensive computer network operations against another State, as well as a private entity empowered to engage in cyber intelligence gathering" is responsible - to whom is the attack attributed?[185]

B. USE OF FORCE

It is undisputed that the prohibition against a "use of force: codified in Article 2(4) of the UN Charter reflects customary international law.[186] But scholars "have struggled mightily to define the threshold at which a [cyber] act becomes a 'use of force'."[187] This

183. *See* TALLINN MANUAL, *supra* note 17, at 32 (suggesting that a state's responsibility for cyber attacks may become rather common under the "effective control").

184. Jeffrey Carr, *Responsible Attribution: A Prerequisite for Accountability*, TALLINN PAPERS, no. 6, 2014.

185. TALLINN MANUAL, *supra* note 17, at 31 (demonstrating the implications of cyber attacks via a corporation on sovereign state, who is then automatically responsible for the actions of the corporation).

186. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 190 (June 27); *see also* Murphy, *supra* note 153, at 43.

187. Schmitt, *Cyber Warfare*, *supra* note 21, at 279; *see also* Marco Roscini, *World Wide Warfare*- Jus ad bellum *and the Use of Cyber Force*, 14 MAX PLANCK Y.B. U.N. L. 85, 90 (2010); Michael N. Schmitt, *Cyber Operations and the* Jus Ad Bellum *Revisited*, 56 VILL. L. REV. 569, 573 (2011); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L

struggle was manifested in the final publication of the TALLINN MANUAL, in which the IGE[188] could not agree upon a consensus bright lined-rule for determining when a cyber operation amounts to a "use of force."[189] They instead adopted the "effects" test, largely based upon the framework set forth in the ICJ's *Nicaragua* decision and Professor Michael Schmitt's effects test framework.[190]

This ambiguity over what level of cyber force would be sufficient to constitute a "use of force" is derived from the fact that Article 2(4)'s prohibition "is both straightforward and ambiguous."[191] It is direct on its face, but "nearly all of its key terms raise questions of interpretation."[192]

The dominant view amongst States is that Article 2(4)'s prohibition applies to military attacks and armed violence.[193] A number of scholars maintain that such an interpretation of Article 2(4) is supported by the plain meaning of the text, as well as other aspects of the UN Charter.[194] This analysis is largely governed by the VCLT, which requires first that the phrase "use of force" be interpreted "in accordance with the ordinary meaning of the phrase with meaning given to that phrase in its context and in light of the Charter's object and purpose."[195] This context may include subsequent practice in the application of the treaty, which establishes

L. 421, 427 (2011).

188. TALLINN MANUAL, *supra* note 17, at x-xiii.

189. *See id.* at 45-48.

190. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 195 (June 27); TALLIN MANUAL, *supra* note 17, at 45 (describing the 'effects' test); Schmitt, *Cyber Warfare*, *supra* note 21, at 279-81.

191. Waxman, *supra* note 187, at 427.

192. Oscar Schachter, *The Right of States to Use Armed Force*, 82 MICH. L. REV. 1620, 1624 (1984) (the restriction of the use of force is ambiguous because the term "force" can be interpreted in different ways).

193. Waxman, *supra* note 187, at 427; Tom J. Farer, Editorial Comment, *Political and Economic Coercion in Contemporary International Law*, 79 AM. J. INT'L L. 405, 408 (1985) (interpreting Article 2(4) as requiring "armed force by one's adversary").

194. Waxman, *supra* note 187, at 428 (adopting the plain meaning of the text viewpoint); Farer, *supra* note 193, at 408 (pointing out various viewpoints of interpretation regarding the meaning of Article 2).

195. Vienna Convention on the Law of Treaties, art. 31(1), May 23, 1969, 1155 U.N.T.S. 331.

the agreement of the parties regarding its interpretation.[196] Recourse may also be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion "in order to confirm the meaning resulting from the application" the VCLT, or to determine the meaning when said interpretation either leaves the "meaning ambiguous or obscure;" or leads to a "result which is manifestly absurd or unreasonable."[197]

Scholars argue that the context of the UN Charter suggests that the phrase "use of force" means "armed" force.[198] The preamble to the UN Charter, for example, sets forth the goal that "armed force" is not to be used "save in the common interest."[199] Likewise, Articles 41 and 42 of the UN Charter authorize the Security Council to take actions not involving armed force and, should those measures be inadequate, to use armed force.[200] Article 51 of the UN Charter also references "armed" attacks.[201]

The drafting history also supports a narrow interpretation of Article 2(4):

> At the San Francisco Conference, the Brazilian delegation submitted amendments to the Dumbarton Oaks proposals that would have extended Article 2(4)'s range to economic coercion. Though the proposition received a majority vote in committee, the Conference declined adopting it by a vote of 26-2. Thus, analysis based on both UN Charter travaux and text leads to an interpretation excluding economic, and for that matter political, coercion from Article 2(4)'s prescriptive sphere.[202]

The issue was raised again "a quarter of a century later during the proceedings leading to the General Assembly's Declaration on Friendly Relations."[203] There, the question of whether "force" should include "all forms of pressure, including those of political or

196. *Id.* art. 31(2)(b).
197. *Id.* arts. 31-32.
198. *See* Schachter, *supra* note 192, at 1624-25; Waxman, *supra* note 187, at 427.
199. U.N. Charter art. 2.
200. *Id.* arts. 41-42.
201. *Id.* art. 51.
202. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 905 (1999) [hereinafter Schmitt, *Computer Network Attack*].
203. TALLINN MANUAL, *supra* note 17, at 46.

economic character, which have the effect of threatening the territorial integrity or political independence of any [s]tate" was "answered in the negative."[204]

In applying Article 2(4) to cyber operations, the IGE found "the focus on scale and effects to be [an equally] useful approach when distinguishing acts that qualify as uses of force from those that do not."[205] The TALLINN MANUAL takes note that "armed" is not necessarily required for a "use of force," relying primarily on the ICJ's *Nicaragua* finding that arming and training a guerrilla force that was engaged in hostilities amounted to an unlawful use of force.[206] This split of debate raises a known unknown—is "armed" force required for a "use of force" under Article 2(4)?

Since State practice is unclear, the IGE adopted an approach to assess whether State cyber operations amount to a use of force. This approach, known as the "Schmitt" test, looks at eight factors to determine whether a cyber operation amounts to a use of force.[207] Developed by Professor Michael Schmitt,[208] these factors include: (1) severity; (2) immediacy; (3) directness; (4) invasiveness; (5) measurability of effects; (5) military character; (6) State involvement; and presumptive legality.[209]

Another known unknown in the use of force context is whether "affording sanctuary (safe haven) to those mounting cyber operations of the requisite severity amounts to a 'use of force' (or 'armed attack')."[210] The majority of the IGE "took the position that in most cases[,] simply granting sanctuary is insufficient to attribute the actions of non-State actors to the State for the purpose of finding a

204. *Id.*; Special Comm. on Friendly Relations and Cooperation Among States (XXIV), Rep. of the Sixth Comm., ¶ 15 (Dec. 4, 1969) (pointing out that the issue of the definition of "force" was still unresolved).

205. TALLINN MANUAL, *supra* note 17, at 45.

206. *Id.* at 46 (citing Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 228 (June 27)).

207. *See id.* at 48.

208. Schmitt, *Computer Network Attack*, *supra* note 202, at 914 (expressing the opinions of Michael N. Schmitt, a professor of International Law at the George C. Marshall European Center for Security Studies in Germany in collaboration with other individuals in the field).

209. TALLINN MANUAL, *supra* note 17, at 48-51.

210. *Id.* at 46-47.

use of force by that State."[211] But they also "did not deem the failure of a State to police its territory in order to prevent the launch of cyber operations to be a use of force[.]"[212] However, the "majority agreed that the provision of sanctuary coupled with other acts, such as substantial support or providing cyber defenses for the non-State group, could, in certain circumstances, be a use of force."[213] Without further State practice on this issue, this is a known unknown.

In the end, there is simply not enough State practice to say, with certainty, what the customary international law requires when it comes to cyber operations and the prohibition against the use of force under Article 2(4) of the UN Charter:

> Over time, the reaction of states to cyber operations, as well as how they characterize their own cyber operations, will inform the process of interpretive maturation. The use of force threshold, wherever it may presently lie, will almost certainly drop in lock step with the increasing dependency of states on cyberspace. Although it is difficult to predict whether any bright-line test will materialize or whether states will simply make use of force characterizations more liberally, a number of options for clarifying the threshold exist.[214]

C. THREAT OF FORCE

Whether a particular cyber operation constitutes a "threat" of force in violation of Article 2(4) of the UN Charter depends upon whether the

> particular use of force envisaged would be directed against the territorial integrity or political independence of a [s]tate, or against the Purposes of the United Nations or whether, in the event that it were intended as a means of defence, it would necessarily violate the principles of necessity and proportionality.[215]

Applied to cyber operations, this would mean that a threat of cyber force would violate the prohibition of Article 2(4) only if the threatened cyber force amounts to an unlawful use of force in the

211. *Id.* at 47.
212. *Id.* at 46-47 (discussing whether granting a safe haven for cyber operations that rise to the requisite severity constitutes a 'use of force').
213. *Id.*
214. Schmitt, *Cyber Warfare*, *supra* note 21, at 279-81.
215. Legality of Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 48 (July 8).

same circumstances. This is the approach endorsed by the scholars, and is the approach followed by Rule 12 of the TALLINN MANUAL.[216]

There are a number of known unknowns in the "threat" context. First, the IGE was "divided as to whether a State manifestly lacking any capability to make good its threat, can violate" Article 2(4).[217] "Similarly no consensus could be achieved regarding a State that possesses the capability to carry out the threat but which clearly has no intention of doing so."[218] These are known unknowns. Likewise, some scholars have argued that a "demonstration of cyber force" could constitute a "threat of force" within the meaning of Article 2(4).[219] Whether this is so remains to be seen.

D. SELF-DEFENSE: ARMED ATTACK

There are at least two areas of "uncertainty with respect to the law of self-defense" that "pose the greatest interpretative potential."[220] The first is ambiguity around whether "a cyber operation that does not result in physical damage or injury can nevertheless amount to an armed attack when it generates severe non-destructive or non-injurious consequences."[221]There was a split of opinion amongst the IGE on this matter.

Some in the IGE adopted a "narrow approach that limited the current law to physical effects."[222] "Others supported an interpretation that focused not on the nature of the consequences (physical), but rather on their severity."[223] Professor Schmitt states the "better view is that, in the absence of conclusive state practice,

216. TALLINN MANUAL, *supra* note 17, at 52.
217. *Id.* at 53.
218. *Id.*
219. *See, e.g.*, Francois Delerue, Emerging Voices: Cyber Operations and the Prohibition of the Threat of Force, Opinio Juris (July 21, 2014, 9:00 AM), http://opiniojuris.org/2014/07/21/emerging-voices-cyber-operations-prohibition-threat-force/ (noting that a demonstration of force can constitute a "second form of threat of force."). This position is particularly notable considering the recent disclosure of the US's Nitro Zeus program.
220. Schmitt, *Cyber Warfare*, *supra* note 21, at 282.
221. *See id.* at 282-83.
222. *Id.* at 283 (excluding attacks which are solely cyber, such as an attack on a state's economic infrastructure).
223. *Id.* (reasoning the damage from a cyber attack, without any physical harm, can be just as damaging, if not more damaging, than the results of a physical attack).

the law of self-defense has not quite evolved to the point where non-destructive or non-injurious cyber operations can qualify as armed attacks."[224] This author agrees. But, as with any area of international law, this known unknown is evolving:

> While future understandings of the notion of armed attack will probably be severity based, how that severity will be measured remains open to question. As with the use of force threshold, the norm could evolve based on certain categories of targets, such as critical infrastructure, that present particular risks of harm or based on various essential activities, like cyber security. Alternatively, severity might be measured in terms of degree of harm, as in the case of economic impact.[225]

A second known unknown in the context of an "armed attack" is "in the relationship between the 'use of force and armed attack thresholds.'"[226] The IGE "took the position that there is a difference between the two." The US has rejected that position: "[T]he United States has for a long time taken the position that the inherent right of self-defense potentially applies against any illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[227]

In short, there have been no international cyber incidents that have been "unambiguously and publicly characterized by the international community as reaching the threshold of an armed attack."[228] This is, by definition, a known unknown.

224. *Id.*
225. *Id.* at 284.
226. Schmitt, *Cyber Warfare*, *supra* note 21, at 284.
227. Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L. J. ONLINE 1, 7 (2012) (agreeing that force should not be defined based on physical force, and further rejecting any standard that would limited a state's ability to defend itself in any type of attack); *see also* Abraham D. Sofaer, *The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 92-96 (1989) (describing the United States' proactive approach to national defense and its inherent conflict with Article 51's wait and respond requirement); William H. Taft, IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE J. INT'L L. 295, 298-300 (2004) (analyzing the United States' argument of self-defense under Article 51 of the U.N. Charter in response to Iran sinking several U.S. vessels).
228. TALLINN MANUAL, *supra* note 17, at 57.

E. SELF-DEFENSE: ANTICIPATORY SELF-DEFENSE?

The law of self-defense has changed dramatically over the last two centuries. During the nineteenth and early twentieth centuries, international law recognized *bellum justum*, which allowed states to resort to violence as a measure of self-help.[229] The Covenant of the League of Nations represented a shift in that discourse, restricting "resort to war" to a limited set of circumstances.[230] The 1928 General Treaty for the Renunciation of War was another major turning point in the development of self-defense rights, reflecting a desire to condemn "recourse to war for the solution of international controversies."[231] This prohibition served as the basis for the creation of Article 2(4) of the UN Charter.[232] Article 51 recognizes an exception to Article 2(4). Although Article 51 of the UN Charter presupposes there is an "armed attack" before a State is permitted to take measures in self-defense, many scholars now believe there is a right to anticipatory, preemptive self-defense.[233]

There are generally two schools of thought on the propriety of anticipatory or preemptive self-defense under international law. First, "the restrictive school argues for a narrow interpretation of self-defence, excluding anticipatory self-defence."[234] This school of thought relies on the plain test of Article 51, which requires the presence of an "armed attack."[235] A number of other scholars support

229. Leo Van den hole, *Anticipatory Self-Defence Under International Law*, 19 AM. U. INT'L L. REV. 69, 70 (2003) (contrasting the traditional notion of *bellum justum* with legal justifications for war).

230. *See* League of Nations Covenant art. 12 (imposing, among other things, a three month waiting period).

231. General Treaty for the Renunciation of War (Kellogg-Briand Pact), art. I, Aug. 27, 1928, 94 L.N.T.S. 57, 59; *see generally* Quincy Wright, *The Meaning of the Pact of Paris*, 27 AM. J. INT'L L. 39 (1933) (discussing the Kellogg-Briand Pact and State's legal obligation to follow the Pact).

232. *See* Van den hole, *supra* note 229, at 71 (explaining that Article 2(4) requires U.N. members to refrain from using force against other states).

233. *See e.g.*, *id.* at 90-91 (noting how the rise of nuclear weapons played a part in the idea of pre-emptive anticipatory self-defense).

234. *Id.* at 80-81 (contrasting with a proactive, anticipatory self-defense approach, as supported by the United States).

235. *See* Van den hole, *supra* note 229, at 81 (citing Josef L. Kunz, *Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations*, 41 AM. J. INT'L L. 863, 878 (1947); BROWNLIE, *supra* note 124, at 244 (noting a lack of consensus on what an armed attack is); Quincy Wright, *The Cuban Quarantine*, 57 AM. J. INT'L L. 546, 560 (1963); Michael J. Glennon, *The Fog of Law: Self-*

the view that customary international law now recognizes a right to anticipatory self-defense in certain circumstances.[236]

The IGE majority "took the position that even though Article 51 does not expressly provide for defensive action in anticipation of an armed attack, a state need not wait idly as the enemy prepares to attack."[237] Instead, a State may defend itself once the armed attack is "imminent." Such action, according to the IGE, would be labeled "anticipatory self-defence."[238] Whether States agree is a known unknown.

Assuming anticipatory self-defense is available, it is also a known unknown whether, and to what degree, the impending attack must be imminent. The IGE acknowledged there are "variations among approaches to anticipatory self-defence."[239] The IGE majority rejected the "strict temporal analysis" of requiring that the "armed attack be about to be launched[.]"[240] Instead, they took "particular note" of the "last feasible window of opportunity" standard.[241] Whether, and to what extent, State practice follows is yet another

Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter, 25 HARV. J.L. & PUB. POL'Y 539, 547 (2002).

236. *See* Van den hole, *supra* note 229, at 81 (citing W.T. Mallison, Jr., *Limited Naval Blockade or Quarantine-Interdiction: National and Collective Defense Claims Valid Under International Law*, 31 GEO. WASH. L. REV. 335, 362-63 (1962-1963)); Derek Bowett, *Reprisals Involving Recourse to Armed Force*, 66 AM. J. INT'L L. 1, 4 (1972) (highlighting the Security Council's differentiation between accepted self-defense and prohibited reprisals during the Armistice Agreements of 1949, and noting that it was "never the intention of the Charter to prohibit anticipatory self defense"); Beth M. Polebaum, *National Self-Defense in International Law: An Emerging Standard for a Nuclear Age*, 59 N.Y.U. L. REV. 187, 201-02 (1984) (suggesting Article 51 needs to be read in broader terms, especially as technology and weaponry are advancing); Schachter, *supra* note 192, at 1633-35; Uri Shoham, *The Israeli Aerial Raid upon the Iraqi Nuclear Reactor and the Right of Self-Defense*, 109 MIL. L. REV. 191, 198 (1985) (supporting anticipatory self-defense and justifying its use in reasonable situations to maintain public order).

237. TALLINN MANUAL, *supra* note 17, at 63.

238. *Id.* at 63-64 (defining imminent as "instant, overwhelming, leaving no choice of means, and no moment for deliberation" as originally stated in the Caroline incident).

239. *Id.* at 64 (differentiating the "about to be launched approach" with the "last feasible window of opportunity approach").

240. *Id.*

241. *Id.* (explaining the last window of opportunity may occur immediately before the attack, or many months before the attack).

known unknown.

F. CYBER RTOP?

There is also a known unknown as to whether, and how, cyber operations could play a role in humanitarian interventions under the auspices of the RtoP doctrine. For example, where a State has information that another State is planning to engage in an act of ethnic cleansing and is doing so by coordinating military action through cyber means, is a State permitted to engage in offensive cyber operations to shut down the control systems, or launch a series of DDoS attacks against the offending State so as to effectuate the RtoP doctrine and protect the citizenry of the sister State? And if such interference would run afoul of the principle of non-intervention, and specifically Article 2(4)'s prohibition against the use of force, would it nonetheless be justified under the RtoP doctrine?

As with many areas of customary international law, it is difficult to ascertain whether the RtoP doctrine, as created by the ICISS report and endorsed by the UN, has reached the level of customary international law. This tension in the law makes clear that whether this area of the law applies to cyber operations is, under any definition of the phrase, a known unknown.

G. ARE THERE PERMISSIVE TYPES OF "COERCIVE" CYBER INTERVENTIONS UNDER INTERNATIONAL LAW?

The principle of non-intervention includes the prohibition on the use of force, as set forth in Article 2(4) of the UN Charter. But the principle of non-intervention also forbids interferences that do not arise to a "use of force," but nonetheless are coercive in nature. The ICJ first dealt with this principle in its *Corfu Channel* decision, and twenty years later, dealt with the issue head on in its 1986 judgment in *Nicaragua*, stating that the "the principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law."[242]

242. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27).

The "precise scope and content of the non-intervention principle remains the subject of some debate."[243] And it is not "clear that all cyber interference automatically violates the international law prohibition on intervention; 'interference pure and simple is not intervention.'"[244] It is therefore the opinion of the TALLINN MANUAL authors that it "follows that cyber espionage and cyber exploitation operations lacking a coercive element do not per se violate the non-intervention principle."[245]

But what remains a known unknown is how cyber operations are to be regulated that are taken in order to coerce and influence individuals to exercise their right to self-determination? Specifically, what happens when a State uses cyber operations to encourage and support a self-determination movement, such as the Arab Spring or an effort by Kurds to create an independent Kurdistan? The right to self-determination is well settled under international law.[246] States generally bear an international obligation "to promote, through joint and separate action, [the] realization of the principle of equal rights and self-determination of peoples."[247] This principle is reflected in substantial State practice, including India's monetary and arms support in 1971 to Pakistani insurgents seeking to create Bangladesh and the UN General Assembly adopting resolutions: (1) condemning self-determination oppression in South Africa and Haiti;[248] (2) calling on the international community to help groups' struggle for self-determination;[249] and (3) recognizing the right to seek and receive

243. TALLINN MANUAL, *supra* note 17, at 44 (proffering that providing funds to insurgents would undoubtedly be considered intervention).

244. *Id.* (noting that instances of coercion will always be wrongful intervention).

245. *Id.*

246. *See* U.N. Charter art. 1(2); G.A. Res. 2105 (XX), Implementation of the Declaration on the Granting of Independence to Colonial Countries and Peoples, ¶ 8, at 4 (Dec. 20, 1965); G.A. Res. 2621 (XXV) Programme of Action for the Full Implementation of the Declaration on the Granting of Independence to Colonial Countries and Peoples, preamble (Oct. 12, 1970); G.A. Res. 2625 (XXV), *supra* note 128, at 122; G.A. Res. 3314 (XXIX), annex, Definition of Aggression (Dec. 14, 1974); Barcelona Traction, Light and Power Company, Limited (Belg. v. Spain), Judgment, 1970 I.C.J. 3, 38-39 (Feb. 5); East Timor (Port. v. Austl.), Judgment, 1995 I.C.J. 90, ¶ 1 (June 30).

247. G.A. Res. 2625 (XXV), *supra* note 128, at 123-24.

248. *See* G.A. Res. S-16/1, Declaration on Apartheid and its Destructive Consequences in Southern Africa, at 4, Dec. 14, 1989).

249. *E.g.*, G.A. Res. 2022 (XX), Question of Southern Rhodesia, 54-55 (Nov. 5,

support in the pursuit of self-determination.[250]

The duties of States to promote self-determination and refrain from violating the territorial integrity or political independence of other States are not mutually exclusive. Both principles coexist on the spectrum of state obligations under international law.[251] The principle of non-intervention could therefore be properly read as a limitation on, but not a complete bar to, a State's obligation to promote and encourage the fulfillment of self-determination rights.[252] Whether States adopt this approach in the context of cyber operations remains to be seen.

IV. CONCLUSION

The foregoing is intended to be descriptive. There are clear principles of the *jus ad bellum* that most likely apply in the cyber context, but there are myriad known unknowns in terms of how said principles should apply. State practice in the offensive use of cyber

1965) (considering the racial discrimination and segregation in South Rhodesia to be a crime against humanity); G.A. Res. 2074 (XX), Question of South West Africa, 60-61 (Dec. 17, 1965) (scolding South Africa for its involvement in South West Africa affairs and requesting South Africa immediately remove itself from South West Africa); G.A. Res. 2189 (XXI), Implementation of the Declaration on the Granting of Independence to Colonial Countries and Peoples, 5-6 (Dec. 13 1966).

250. *See* G.A. Res. 2625 (XXV), *supra* note 128, at 122-24 (detailing the rights of all peoples and states); G.A. Res. 3314 (XXIX), *supra* note 246, at 143 (defining "aggression" that falls outside the scope of international peace); G.A. Res. 42/44, Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, 2-4 (Nov. 18, 1987).

251. *See, e.g.*, G.A. Res. 1514 (XV), Declaration on the Granting of Independence to Colonial Countries and Peoples, 66-67 (Dec. 14, 1960) (distinguishing self-determination and political integrity as two separate entities with different objectives); G.A. Res. 2625 (XXV), *supra* note 128, at 123-24 (repeating the phrase "joint and separate action"); U.N. Charter art. 1; OSCE, *supra* note 135, at 7 (suggesting self-determination is an inherent right and territorial integrity is an established norm of international law).

252. *See, e.g.*, Western Sahara, Advisory Opinion, 1975 I.J.C. 12, 100-102 (Oct. 16) (analyzing the territorial sovereignty of Western Sahara from the kingdom of Morocco in anticipation of Western Sahra's decolonization); Accordance with International Law of Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, 2010 I.C.J. 403, 436-52 (July 22) (assessing whether Kosovo's declaration of independence was in accordance with international law despite its conflict with a Security Council resolution).

operations is increasing, and there will undoubtedly be more clarity in this area of the law with the passage of time.