Cleveland-Marshall
College of Law Library

Cleveland State Law Review

Volume 63
Issue 2 *Symposium: American Education: Diversity, Desegregation, and Resegregation*

Article 12

2015

Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict,: A NATO-Centric Approach

Terence Check

Follow this and additional works at: https://engagedscholarship.csuohio.edu/clevstlrev

 Part of the International Law Commons, and the Military, War, and Peace Commons

How does access to this work benefit you? Let us know!

Recommended Citation

Terence Check, *Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict,: A NATO-Centric Approach*, 63 Clev. St. L. Rev. 495 (2015)
available at https://engagedscholarship.csuohio.edu/clevstlrev/vol63/iss2/12

This Article is brought to you for free and open access by the Journals at EngagedScholarship@CSU. It has been accepted for inclusion in Cleveland State Law Review by an authorized editor of EngagedScholarship@CSU. For more information, please contact library.es@csuohio.edu.

BOOK REVIEW

ANALYZING THE EFFECTIVENESS OF THE TALLINN MANUAL'S JUS AD BELLUM DOCTRINE ON CYBERCONFLICT, A NATO-CENTRIC APPROACH

Review of TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. By MICHAEL SCHMITT ED. New York: Cambridge University Press. 2013. Pp. 304. $129.99.

TERENCE CHECK*

I. INTRODUCTION

The advent of computer technology has changed the way society communicates, conducts business, and wages war. But despite the increasingly martial nature of the computer, the law of armed conflict (also known as international humanitarian law) has yet to react to the destructive nature of computer-based conflict. While the wider lay public has begun to recognize and fear the enemy at the other end of the fiber-optic cable, cyberattacks have captured the imaginations of politicians, generals and pop culture,[1] not everyone agrees on

* Law & Government Fellow, American University; JD, Cleveland-Marshall College of Law, Cleveland State University. Terence would like to thank his awesome family and his fiancée Monica for their support and inspiration. The views and opinions expressed herein are solely those of the author, and do not represent American University, Cleveland-Marshall College of Law, or any other person or entity.

[1] *See, e.g.*, SKYFALL (Eon Productions 2012) (depicting the classic Bond villain as a maniac who is able to carry out sophisticated and destructive cyberattacks); CALL OF DUTY: BLACK OPS II

Published by EngagedScholarship@CSU, 2015

cyber war's importance,[2] or even its existence. This complicates any strategic approach to dealing with cyber-security as the disagreements in the technical and legal discourse hinder the decision-making process. Some commentators state that there may be no "cyberwar,"[3] or that any "cybertreaty" is unnecessary,[4] or that existing norms are "good enough."[5] Answers to lingering questions about how malware affects conflict resolution, jus ad bellum and jus in bello need to be answered before computer technology compels a response from the legal community. The current state of law pertaining to "cyberwarfare"[6] is still undeveloped and ambivalent on many issues.[7]

Even if one hesitates to characterize a cyberattack as an armed attack,[8] the chaotic nature of cyberconflict demands attention, and the hawkish nature of politicians and military leaders regarding cybersecurity lends a desperate urgency to the conflict.[9] To complicate matters, international discourse often fixates on the contents of the cyber security lexicon.[10] Similar attention is paid to civic issues like

---

(Activision 2012) (using a global cyberattack as the major plot point); Lance Whitney, *U.S. General Warns of Iran's Growing Cyber Strength*, CNET NEWS (Jan. 18, 2013), http://www.cnet.com/news/u-s-general-warns-of-irans-growing-cyber-strength/; Deborah Charles, *U.S. Homeland Chief: Cyber 9/11 Could Happen "Imminently,"* REUTERS (Jan. 24, 2013), http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.

[2] Jason Healey, *No, Cyberwarfare Isn't as Dangerous as Nuclear War*, U.S. NEWS & WORLD REPORT (Mar. 20, 2013), http://www.usnews.com/opinion/blogs/world-report/2013/03/20/cyber-attacks-not-yet-an-existential-threat-to-the-us.

[3] *Cyber War May Never Take Place*, KING'S COLL. LONDON (Oct. 10, 2011), http://www.kcl.ac.uk/newsevents/news/newsrecords/2011/10October/Cyber-war-might-never-happen.aspx.

[4] Sean Lawson, *Cyberwarfare Treaty Would Be Premature, Unnecessary and Ineffective*, U.S. NEWS & WORLD REPORT (June 8, 2012, 4:14 PM), http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare/cyberwarfare-treaty-would-be-premature-unnecessary-and-ineffective.

[5] *NATO Official: Existing Rules for Global Cyberdefense Good Enough*, 27 INSIDE THE PENTAGON, no. 13, Mar. 31, 2011, http://insidedefense.com (on file with author).

[6] Understandably, this is a contentious term. See *infra* note 10 for a brief discussion of the cyber-security lexicon.

[7] For example, the United States Department of Defense makes no mention of how the norms of the Laws of Armed Conflict (LOACs) apply to cyberspace. *See generally* U.S. DEP'T OF DEF., DEP'T OF DEF. STRATEGY FOR OPERATING IN CYBERSPACE (2011), http://www.defense.gov/news/d20110714cyber.pdf.

[8] As contemplated by Article 51 of the U.N. Charter. *See* U.N. Charter art. 51.

[9] Jordan Chandler Hirsch & Sam Adelsberg, *An Elizabethan Cyberwar*, N.Y. TIMES, May 31, 2013, http://www.nytimes.com/2013/06/01/opinion/an-elizabethan-cyberwar.html?pagewanted=all&_r=0 ("This emergence of cyber hawks in both nations raises the odds of a hack becoming a cyberwar. These voices could pressure both nations to treat any escalating cyberconflict as a latter-day Cuban missile crisis.").

[10] Daniel J. Ryan, Maeve Dion & Eneken Tikk, *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161, 1166-67 (2011); *see also* Jeffrey Carr, *What is Cyberwar?*, SLATE (Aug. 12, 2011), http://www.slate.com/articles/technology/future_tense/2011/08/what_is_cyberwar.html ("U.S. Senators have complained recently that

citizens' freedom and privacy in cyberspace.[11] One of the recent major developments in the law of armed conflict is the Tallinn Manual.[12] The Manual represents one of the first documents devoted solely to exploring how events in cyberspace happen affect the operation of the law of armed conflict.[13] Naturally, the Manual is limited in scope because very few cyberattacks would be of the nature and severity to prompt an analysis under the laws of armed conflict.[14] But it is precisely these sorts of attacks that give form to the fears of policymakers. This review will analyze the effectiveness of the Tallinn Manual in answering the question of how international humanitarian law deal with cyber warfare, and whether there are any usable norms that organizations like NATO could employ in responding to a cyber attack.[15]

This review folds out in four parts. While the problem of cyberconflict has been briefly introduced in Part I, the forthcoming pages will highlight the vexing legal issues posed by hackers, cyber soldiers, and malware. In Part II, this Review will present a brief background on NATO to give the reader a slight background on the history and structure of that organization, especially since NATO (and its Cooperative Cyber Defense Center of Excellence ("CCDCOE")) played a large role laying the groundwork in the composition of the Manual. In addition, Part II will discuss prevailing trends in the cybersecurity/"cyberwar" law to help illustrate the salience of the issue and the role that NATO fills in the global security community, which will show why the Tallinn Manual is so important to this global discussion.

In Part III, the Tallinn Manual's sections on jus ad bellum will be evaluated to see how adequately it determines where cyberattacks fall within the "armed

---

there's still no clarity on what . . . would be considered an act of cyberwar.") ("Howard Schmidt, the U.S. Cyber-Security Coordinator . . . said in an interview with *Wired* that 'there is no cyberwar.'"). Laypersons frequently use terms like "cyberwarfare" with remarkable imprecision. *See, e.g.*, Grant Brunner, *US Congress: China's Cyberwarfare is Becoming a Serious Problem for the United States*, EXTREME TECH (Nov. 7, 2012, 10:54 AM), http://www.extremetech.com/extreme/139722-us-congress-china-cyberwarfare-is-becoming-a-serious-problem-for-the-united-states ("A draft report from the U.S. Congress shows that Chinese cyberwarfare is a growing issue that leaves the United States vulnerable in a very serious way."). There is no indication that the Chinese have engaged in any behavior that would constitute an armed attack. For an example of the misuse of the word "cyberattack," see Paul Hales, *Russians Launch Cyber Attack on Lithuania: Media Reports*, SC MAGAZINE (July 1, 2008, 10:03 AM), http://www.scmagazine.com.au/News/115647,russians-launch-cyber-attack-on-lithuania-media-reports.aspx.

[11] This is a tangential issue because the potential loss of liberty is a civil issue, one for resolution by individual nations/governments. Insofar as the LOAC and a NATO policy response is developed, the issue of civil liberty is one not appropriate for discussion here. As the field of LOAC for cyberspace develops, then discussion of reconciling security laws and civil liberties may be a field relevant for discussion.

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

[13] *Id.*

[14] *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 822 (2012).

[15] TALLINN MANUAL, *supra* note 12, at 11. The Manual is not fully or officially endorsed by NATO, but nevertheless its roots are borne out of the Alliance through NATO's Collective Cyber-Defense Center of Excellence.

attack"/"illegal use of force" paradigm. Particular attention will be paid to whether the doctrine of the manual is (1) sufficiently cognizant of the theoretical underpinnings of the law of war (what does the law of war seek to achieve), and (2) how well the doctrinal rules of the Manual can be used in practical situations. Following this analysis, this article will evaluate the Manual's shortfalls.

To briefly foreshadow, it is often the case that new legal works sometimes fall short, even though its drafter(s) are exceedingly qualified and its intentions are pure. The Tallinn Manual is one such work. While the doctrinal rules of the Manual are a solid first step towards articulating new rules for an age of cyber warfare, there are some fundamental problems. The Manual is at times divorced from the theoretical foundations of the law of war and how the Manual's rules will operate in a practical setting. Even though the manual is an imperfect guide, it is this Author's conclusion that something is better than nothing.

II. BACKGROUND

A. The NATO Charter and its Subsequent Redirections

NATO was founded in 1949[16] near the outset of the Cold War. Its primary purpose was to organize the collective defense of Western Europe, contemplating an eventual armed struggle with the military forces of the Soviet Bloc and the contemporaneously formed Warsaw Pact.[17] But NATO was far from a regional partisan organization. The Washington Treaty, which brought the Alliance into existence, enshrines many of the principles of the United Nations Charter[18]and even gives deference to the United Nations Security Council[19] within key articles of the treaty.[20]

---

[16] *See* North Atlantic Treaty art. 1, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243 [hereinafter NATO Treaty] (founding of NATO was based on the adoption of this treaty).

[17] NATO, *A Short History of NATO*, http://www.nato.int/history/nato-history.html (last visited Oct. 15, 2014) (listing Soviet aggression and expansionism as one of the main reasons for the formation of the Alliance, as well as the suppression of nationalist militarism and the encouragement of European political integration and cooperation).

[18] NATO Treaty, *supra* note 16, at art. 1 ("The Parties undertake, as set forth in the Charter of the United Nations, to settle any international dispute in which they may be involved by peaceful means . . . .").

[19] It is interesting to note that provisions relating to peacekeeping action of the United Nations Security Council (UNSC) given the composition of the Council. It seems unlikely that the UNSC would be able to form the necessary agreements to take action in *any* regard, let alone in a geographic area where Cold War tensions were high and military conflict was contemplated (hence the creation of NATO).

[20] *See* NATO Treaty, *supra* note 16, at art. 5 ("[A]ll measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."). These principles are again a curious indication of the spirit of international security and multilateralism that NATO purports to uphold as noted in note 29. It is unlikely, however, that the Allies would have borne the political cost of repudiating the Chapter VII powers of the U.N. Charter in order to circumvent the shifting of responsibility when the conditions needed in order to perform such a shift would never arise during the Cold War.

Article 5 is the most important of all the articles of the Washington Treaty as it sets forth NATO's primary operational and legal mandate. It reads:

> [T]he Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area . . . .[21]

In summary, Article 5 provides that if any member suffers an attack, all other members shall respond as if the attack was directed against them personally. This article multiplies the deterrent capabilities of all of the NATO member nations: not only does each nation gain the strength of the other members, but smaller nations can use the entire Alliance and its capabilities as a whole to shield[22] against threats to their national security.

But no mere act of force[23] will trigger the activation of Article 5: Only an "armed attack"[24] will do. Thus, simple acts of force, (including economic force and other coercive measures) would not meet the Article 5 threshold.

No simple armed attack will do either, because small border actions or a skirmish would not trigger the activation of Article 5.[25] Even if one NATO member nation pushed for the invocation of Article 5,[26] the relevant text of the treaty is nevertheless permissive: NATO member nations are not compelled to do anything beyond "such action as it deems necessary."[27] In marked contrast to a small armed incident, the terrorist attacks of September 11, 2001 were met with a collective response under Article 5.[28] NATO adopts this approach because it seeks to minimize threats to the

---

[21] NATO Treaty, *supra* note 16, at art. 5.

[22] For example, the Baltic States (Estonia, Latvia, Lithuania) rely and depend on NATO to secure their territorial integrity vis-à-vis air patrols. *See Baltic Air Policing*, WIKIPEDIA, http://en.wikipedia.org/wiki/Baltic_Air_Policing (last visited Dec. 8, 2014).

[23] For contrast, compare the language of the U.N. Charter's blanket prohibition on the use of force in U.N. Charter art. 2(4).

[24] *See* NATO Treaty, *supra* note 16, at art. 5.

[25] *See Turkey to Push NATO to Consider Syria's Downing of Turkish Jet as Attack on Military Alliance*, FOXNEWS.COM, June 25, 2012, http://www.foxnews.com/world/2012/06/25/ syria-fires-at-second-turkish-plane-deputy-prime-minister-says/ ("Turkey will push NATO to consider the jet's downing under Article 5 in a key alliance treaty. Article 5 states that an attack against one NATO member shall be considered an attack against all members.").

[26] *Id.* ("Asked if Turkey will insist on the activation of Article 5 of NATO, Arinc [the deputy prime minister of Turkey] said, 'No doubt, Turkey has made necessary applications with NATO regarding Article 4 and Article 5.'").

[27] *See* NATO Treaty, *supra* note 16, at art. 5.

[28] *See* Edgar Buckley, *Invoking Article 5*, NATO REVIEW (Summer 2006), http://www.nato.int/docu/review/2006/issue2/english/art2.html ("Canadian Ambassador

entire North Atlantic region and as a result, a high threshold of the use and impact of force is implied in Article 5.[29]

But the Washington Treaty is not a static document. The drafters of the treaty recognized that the security environment of the Transatlantic Region may change, and, as a result, built the opportunity for periodic review into the treaty itself.[30] While amending the treaty outright has only occurred in a few instances,[31] the Alliance has developed a unique way to reformulate Alliance-wide strategy without editing the Treaty's text through the drafting and adoption of "Strategic Concepts," which are documents that capture the Alliance's current operational and dynamic view of the NATO Charter.[32] Each Strategic Concept, drafted by a group of experts, outlines and defines what security issues are important to NATO, and how to deal with those security issues in a wider geopolitical context.[33]

To transition into a new age of warfighting, NATO has sought to create means of supplementing and supporting Alliance members by pooling resources and enhancing cooperation between nations,[34] but has yet to devise a way to bind the members to a common course of development, especially in the field of cyberconflict. Given NATO's encounters with cyberconflict[35] and its endemic political difficulties,[36] the Alliance needs to develop a mechanism to institute clear

---

David Wright . . . who was also dean of the Council, assured him of the support of all the Allies. 'Hell, this is an Alliance,' he said. 'We've got Article 5.'").

[29] *Id.* ("The scale was important, we felt, because the Washington Treaty had been written to deal with threats to peace and security in the North Atlantic area, which implied a high threshold of the use or impact of force.").

[30] NATO Treaty, *supra* note 16, at art. 13.

[31] Ulf Haußler, *Cyber Security and Defence From the Perspective of Articles 4 and 5 of the NATO Treaty*, *in* INTERNATIONAL CYBER SECURITY LEGAL & POLICY PROCEEDINGS 100, 108 (Cooperative Cyber Defense Center of Excellence ed., 2010), *available at* http://www.ccdcoe.org/publications/legalproceedings/Haussler_CDfromArticles4and5Perspective.pdf ("The attack on the United States of America on 11 September 2001 (hereinafter referred to as '9/11') represents the only case in which NATO's collective self-defence mechanism was used.").

[32] Jens Ringsmose & Sten Rynning, *Come Home, NATO? The Atlantic Alliance's New Strategic Concept*, 6 DANISH INST. FOR INT'L STUDIES, , DIIS REPORT (Danish Inst. for Int'l Studies, Copenhagen, Den.), *available at* http://www.econstor.eu/bitstream/10419/59829/1/593489322.pdf.

[33] *Id.* ("[T]he Strategic Concept must specifically interpret concrete geopolitical circumstances.").

[34] Press Release, NATO, Summit Declaration on Defence Capabilities: Toward NATO Forces 2020 (May 20, 2012), http://www.nato.int/cps/en/natolive/official_texts_87594.htm?mode=pressrelease.

[35] *See infra* Part II(B).

[36] Nowhere else is this frustrating (perhaps even toxic) divergence of national interests more apparent than in the case of the potential accession of the Former Yugoslav Republic of Macedonia (FYROM). *See* Karl-Heinz Kamp, *NATO Enlargement Reloaded*, 81 RESEARCH PAPER (Research Division – NATO Defence College, Rome, Italy), Sept. 2012, at 2, *available at* http://www.ndc.nato.int/download/downloads.php?icode=349 ("Other Allies, particularly the United States, are becoming increasingly impatient with the Greek obstructionism . . . .").

legal norms that can serve as guidelines to NATO personnel, agencies, and its member nations. Perhaps the Tallinn Manual can guide the Alliance in a rapidly developing world of cyberconflict and information warfare.

B. NATO's Encounters with Cyberwarfare

The operational and legal needs of the North Atlantic Treaty Organization and its member nations concerning cyberconflict are unique and specific.[37] Yet for an organization tasked with ensuring the defense of the Transatlantic Region,[38] it continues to have difficulties[39] in modernizing and updating its operational capabilities.[40] These difficulties manifest themselves in the hurried development of NATO facilities designed to combat the role of cyber-threats.

In 1999, NATO became concerned with the security of its military information networks after the websites of Supreme Headquarters Allied Powers Europe ("SHAPE") and other NATO entities were targeted by Denial of Service ("DOS") attacks[41] during the conduction of NATO's Operation Allied Force[42] (NATO's air operations against Yugoslavia during the Kosovo War). Growing out of this set of initial attacks, NATO adopted the Cyber Defense Program ("CDP") at the 2002 Prague Summit.[43] In the years immediately after the adoption of the CDP, there was little progress in developing NATO's cyberdefence capabilities.

This changed in 2007. That year, the Republic of Estonia, a member-nation of NATO, experienced a massive Distributed Denial of Service ("DDOS") attack that

---

If NATO (as a whole) is subject to the whims of one nation-state on a relatively non-controversial issue, then the Alliance's ability to exercise effectively in contested areas of policy or during a crisis is naturally in question.

[37] *See* NATO Frequently Asked Questions, http://www.nato.int/cps/en/natolive/faq.htm (last updated Mar. 11, 2009).

[38] Davis Brown, *The Role of Regional Organizations in Stopping Civil Wars*, 41 A.F. L. REV. 235, 242-43 (1997).

[39] The fiscal difficulties in upgrading military equipment and infrastructure that face the Alliance are all the more apparent, as according to 2011 estimates, on average, NATO countries spend only 3.8 percent of their defense budgets on infrastructure maintenance. *See* Press Release, NATO, Financial and Economic Data Relating to NATO Defence (Apr. 13, 2012), http://www.nato.int/nato_static/assets/pdf/pdf_2012_04/20120413_PR_CP_2012_047_rev1.pdf. By looking at this report, many Alliance neophytes spend more than sixty percent of their annual defense budgets on personnel and retirement costs.

[40] *See* Fahad Ullah Khan, *States Rather Than Criminals Pose a Greater Threat to Global Cyber Security: A Critical Analysis*, 31 STRATEGIC STUDIES 91, 91, (2011), *available at* http://issi.org.pk/wp-content/uploads/2014/06/1328592265_43276030.pdf.

[41] Jason Healey & Klara Tothova Jordan, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, ATL. COUNCIL OF THE U.S., Sept. 2014, at 1, *available at* http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf.

[42] Operation Allied Force was an aerial bombardment campaign conducted in order to force military units of the Federal Republic of Yugoslavia from Kosovo. *See Operation Allied Force*, U.S. DEP'T OF DEF., http://www.defense.gov/specials/kosovo/ (last visited June 19, 2013).

[43] *Id.*

crippled the nation's information networks, media outlets, and the entire nation's financial sector.[44] The attack lasted for almost a month, and the frequency and ferocity of the attacks was unprecedented. As a result, the Cooperative Cyber-Defence Centre of Excellence ("CCDCOE") and the Cyber Defense Management Agency ("CDMA") were founded in 2008.[45] The most recent Strategic Concept,[46] adopted in November 2010, outlined the importance of NATO's role in contributing to cybersecurity.[47] NATO 2020, a policy report published by the NATO Group of Experts[48] in preparation for the release of the 2010 NATO Strategic Concept, named cyberattacks of varying degrees of severity as the third greatest threat to the security of the Alliance.[49]

Yet, the development of NATO's cyberdefence forces is not without its challenges. The CCDCOE (located in Tallinn, Estonia) is staffed by less than fifty personnel and it is located in a repurposed army barracks dating back to the Tsarist era.[50] Only eleven of the twenty-eight NATO allies are participants in the CCDCOE.[51] This may indicate a lack of political will in committing to cyberdefence research and may show a reluctance to embrace new international norms.

C. Other Viewpoints on Cyber-Warfare

Other major powers diverge on what security in cyberspace should entail. On one hand, Russia and China are concerned with "information security," choosing to focus on what information is protected and how it can be protected, while the more

---

[44] Sverre Myrli, NATO and Cyber Defence, NATO Parliamentary Assembly, 173 DSCFC 09 E BIS (2009).

[45] *Id.*

[46] The Strategic Concept is an assessment that outlines the broad strategic objectives for NATO for the period following its adoption. *See* NATO, *NATO's New Strategic Concept*, http://www.nato.int/strategic-concept/ (last visited Dec. 8, 2014).

[47] NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*, ACTIVE ENGAGEMENT, MODERN DEFENCE (NATO Summit, Lisbon, Portugal), Nov. 19-20, 2010, at 11, 16-17, *available at* http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf.

[48] For more information on the NATO Group of Experts, see NATO, *Group of Experts*, http://www.nato.int/strategic-concept/experts-strategic-concept.html (last visited Sept. 9, 2014).

[49] *NATO 2020: Assured Security; Dynamic Engagement*, GROUP OF EXPERTS (NATO Summit Report, Lisbon, Portugal), May 17, 2010, at 17, *available at* http://www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

[50] Valentina Pop, *Estonia Training NATO 'Techies' for Cyberwar*, EUOBSERVER.COM (June 14, 2011, 9:29 AM), http://euobserver.com/cyber/32479. To add to the institutional frustrations, the CCDCOE, though it is a part of NATO's wider educational framework managed by Allied Command Transformation (ACT), is not a part of NATO's command structure. All Centers of Excellence (COEs) are considered international military organizations. *See* NATO, *Centres of Excellence*, http://www.nato.int/cps/en/natolive/topics_68372.htm (last visited Aug. 26, 2012).

[51] Press Release, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), Netherlands Joins the Centre (Apr. 5, 2012), http://www.ccdcoe.org/netherlands-joins-centre.html.

"Western" approach opts to focus on a model of "cyberspace security" which places the security and integrity of networks and information infrastructure as the primary area of concern.[52] Another viewpoint comes from Fahad Ullah Khan, a Research Fellow at Pakistan's Institute of Strategic Studies Islamabad ("ISSI"). Fahad states that cybersecurity should not focus on whether state-based attacks or criminal attacks are more threatening to global security; rather, Khan outlines the need for legal guidelines to govern all types of attacks within cyberspace.[53] He notes that a simple technical solution to the cybersecurity problem is inadequate[54]—without enforceable rules and norms, perpetrators (state or individuals) will not be deterred from strategically mounting cyberattacks in the long term.[55]

In terms of technical development, the field of cybersecurity is one of dynamism. Iran, a recent victim of a robust cyberattack,[56] has started a "cyber-warfare" initiative that is designed to counter cyberattacks that use malware and viruses like Stuxnet and Duqu,[57] rumored to have sparked the development of an expensive Iranian cyberwarfare program.[58] These are examples of the growing amount of focus, attention, and money that states are devoting in order to defend their vital information networks.

In some cases, the actions of states go beyond simple defense. Embattled regimes can use the tactics of cybercriminals and cyberattackers to suppress rebel or dissident movements within their nations. In Syria, the Assad regime has taken advantage of the fact that the government controls the country's information networks, and has used such control to hack into rebel computers and mobile phones.[59] This aspect of Syrian conflict indicates a fundamental truth: that a cyber-savvy opponent can be as much of an asymmetric threat as its purely conventional counterpart. If skills in

---

[52] Adam Segal, *The Role of Cyber-Security in US-China Relations*, EAST ASIA FORUM (June 21, 2011), http://www.eastasiaforum.org/2011/06/21/the-role-of-cyber-security-in-us-china-relations/.

[53] *See generally* Khan, *supra* note 40 (declining to analyze the overall importance of cybercrime in the face of more geopolitically pressing issues related to cybersecurity).

[54] *See id.* at 102.

[55] *Id.* at 103.

[56] Gary Brown, *Why Iran Didn't Admit Stuxnet was an Attack*, 63 JOINT FORCE QUARTERLY 70, 70 (Oct. 1, 2011), *available at* http://www.academia.edu/4237109/Why_Iran_Wont_Admit_Stuxnet_Was_an_Attack.

[57] Stuxnet was a computer worm designed to target supervisory control and data acquisition (SCADA) systems in computers produced by German technology company Siemens. *See SCADA*, WIKIPEDIA, http://en.wikipedia.org/wiki/SCADA (last visited June 3, 2014). Duqu is a variant of the original Stuxnet worm, but instead of causing damage like Stuxnet, Duqu is designed to infiltrate and gather information on system vulnerabilities. *See Duqu*, WIKIPEDIA, http://en.wikipedia.org/wiki/Duqu (last visited Jan. 15, 2015). *See* David Shamah, *Top Security Exec: Beware the 'Sons of Stuxnet,'* THE TIMES OF ISRAEL (June 3, 2013 2:41 PM), http://www.timesofisrael.com/top-security-exec-beware-the-sons-of-stuxnet/.

[58] Yaakov Katz, *Iran Embarks on $1B. Cyber-Warfare Program*, THE JERUSALEM POST (Dec. 18, 2011), http://www.jpost.com/Defense/Iran-embarks-on-1b-cyber-warfare-program.

[59] Jay Newton-Small, *Hillary's Little Startup: How the U.S, Is Using Technology to Help Syria's Rebels*, TIME (June 13, 2012), http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/.

cybersecurity can enable dissidents, protestors, and rebels to maximize their tactical capabilities, the same naturally follows for smaller nations with small militaries.

The Syrian situation, however, is unique in that the government controls a large portion of the information networks.[60] In the West, private companies own more than eighty percent of the information infrastructure, and those companies do not collaborate with their governments on cybersecurity.[61] One reason civilian networks are now a concern is because programmable logic controllers ("PLCs")[62] (predominantly owned and operated by civilian and private sector entities) can be damaged or destroyed by cyberattacks, and as a result may cripple many vital governmental and quasi-governmental services. Security and law are no longer separate disciplines.[63]

III. DISCUSSION

A. The Drafters of the Tallinn Manual

The Drafters of the Tallinn Manual constitute a group of well-qualified experts hailing from many nations, including the United States, Canada, Australia, Belgium, the Netherlands, the United Kingdom, and Sweden.[64] Collectively, these experts are referred to as the "International Group of Experts."[65] This independent group is the entity responsible for the drafting of the Tallinn Manual.

B. The Scope and Effect of the Tallinn Manual

In response to the widespread institutional and international confusion on where to place acts of cyber warfare within the Law of Armed Conflict, the CCDCOE invited the International Group of Experts to draft a manual addressing the confusion vis-à-vis "cyberwar."[66] The CCDCOE, however, is not a part of NATO's overarching command structure, it receives no funding from NATO, and though each operational center is "accredited" by NATO, member nations must sign memoranda of understanding ("MOU") in order to join in a center's operations.[67] As

---

[60] *Id.*

[61] *See generally* Khan, *supra* note 40 (noting that the lack cooperation between the private sector and the government in the area of cybersecurity poses security threats).

[62] PLCs are parts of SCADA systems, which are critical to modern infrastructure systems like water purification plants. *See SCADA*, *supra* note 61.

[63] *March of the Robots*, THE ECONOMIST, June 2, 2012, at 13, *available at* http://www.economist.com/node/21556103.

[64] TALLINN MANUAL, *supra* note 12, at x-xiii.

[65] *Id.*

[66] *Id.*

[67] NATO, *Centres of Excellence*, http://www.nato.int/cps/en/natolive/topics_68372.htm (last visited Aug. 26, 2012) ("Although not part of the NATO command structure, they are part of a wider framework supporting NATO Command Arrangements . . . . Once ACT approves the concept, the COE and any NATO country that wishes to participate in the COE's activities then negotiate two Memorandums of Understanding (MOU) . . . . The Alliance does not fund COEs. Instead, they receive national or multinational support, with "Framework Nations", "Sponsoring Nations" and "Contributing Nations" financing the operating costs of the institutions.").

a result, the Tallinn Manual is like other legal manuals regulating warfare on the sea and in the air—it is a well crafted, but nonetheless non-binding legal document.[68]

But the Tallinn Manual promises to impact future legal development despite its non-binding effects. It analyzes cyberattacks through the lens of international humanitarian law, paying attention to how jus ad bellum and jus in bello are applied to acts within cyberspace. Like this article, the Tallinn Manual pays little attention to traditional constitution of electronic warfare or issues like intellectual property theft, espionage, or other cybersecurity issues that do not warrant an international humanitarian law analysis,[69] especially under jus ad bellum.[70]

C. The Composition of the Tallinn Manual

According to the online manuscript,[71] the Tallinn Manual is divided into two parts: Part A (a discussion of international cyber security law, but really pertaining to jus ad bellum), and Part B (a discussion of the law of cyber armed conflict/jus in bello).[72] Between the two parts, there are seven chapters that pertain to subjects such as state acts in cyberspace, the protection of specific classes of persons, and the applicability of the law of armed conflict to acts within cyberspace.[73] Within the seven chapters, there are ninety-five rules that articulate the International Group of Experts' views on a wide range of legal issues.[74]

Although many of the Manual's rules are prospective and extremely specific, it is unclear whether a situation would ever arise where these specific rules would be needed to determine the legal repercussions of a cyberattack on medical vehicles, equipment or personnel.[75] Regardless of whether a cyberattack would actually be directed against the aforementioned targets, such an act would be regulated by already standing norms of International Humanitarian Law.[76] Thus, much of the

---

[68] TALLINN MANUAL, *supra* note 12, at 11. This point is clearly articulated in the following statement: "The Manual does not represent the views of the NATO CCD COE, its sponsoring nations, or NATO. In particular, it is not meant to reflect NATO doctrine." *Id.*

[69] *Id.* at 4.

[70] Unlike entities like the European Union (for example), NATO has no operational (or legal) mandate to delve into policymaking on civilian or domestic cybersecurity issues. *See* Alexander Klimburg & Heli Tirmaa-Klaar, CYBERSECURITY AND CYBERPOWER: CONCEPTS, CONDITIONS AND CAPABILITIES FOR COOPERATION FOR ACTION WITHIN THE EU, EUROPEAN PARLIAMENT (Directorate-General for External Policies of the Union, Wiertz, Brussels (2011), at 26-27. As a result, NATO's role has been one of facilitator, not policymaker. *See id.*

[71] The TALLINN MANUAL can be found online. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, http://issuu.com/nato_ccd_coe/docs/tallinnmanual.

[72] The discussion of cyber armed conflict deals with various issues such as respecting neutrality (Chapter VII), specific rules on targeting protected persons like children, clergy, journalists, etc. (Chapter V), and general rules for the conduct of hostilities (Chapter IV). *Id.* at vi-xi. In this regard, the TALLINN MANUAL is little more than text that applies "traditional" International Humanitarian Law. *See id.*

[73] TALLINN MANUAL, *supra* note 12.

[74] *Id.*

[75] *Id.* at 204-05.

[76] This principle is actually illustrated by the TALLINN MANUAL itself. *See id.*

Tallinn Manual's jus in bello analysis[77] seems to be nothing more than a reiteration of the general applicability of the law of war to cyberattacks and cyberwarfare.[78] The most contentious issues discussed by the Manual are not how a cyberwar should be fought, but rather how to identify and how to respond to the start of a cyberwar.

D. Discussing the Adequacy of the Tallinn Manual: Did the Drafters Leave Gaps?

Part A of the Tallinn Manual discussed the jus ad bellum of cyberconflict. As a political and military alliance that must conduct itself in accordance with international law, what should concern NATO is whether the Tallinn Manual's jus ad bellum analysis is lacking in any significant respect. Simply put, do the ninety-five black letter rules of the Manual leave gaps that can exploited by those who seek to make war via cyberspace? How well does the doctrine of the Manual consider the theoretical goals of jus ad bellum while still considering the practical application and operation of the Manual's "Rules"? To answer this question, this article will consider the Manual's major jus ad bellum provisions: Rule 9, Rule 10, Rule 11, and Rule 13.

1. Rule Nine: Countermeasures

Rules Six, Seven and Eight outline some norms for attributing cyberattacks in rather ordinary fashion.[79] These rules establish that the mere fact alone that a cyberattack originates in a state's territory and/or that a cyberattack is routed through a state's cyber infrastructure is not enough to attribute that attack to the state in question.[80] Rule Nine regulates a victimized state's potential countermeasures to a cyber operation. The rule states that: "[a] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[81] The International Group of Experts note that this rule is little more than an extension of the customary international law articulated in the International Law Commission's ("ILC") Articles on State Responsibility.[82] In addition to the limits imposed on State countermeasures, the Group of Experts notes that when the exact nature or responsible party of a cyber attack cannot be ascertained, a state could nevertheless employ countermeasures based on the plea of necessity.[83] Substantively, one can conclude that NATO's

---

[77] The *jus in bello* analysis comprises Part B of the TALLINN MANUAL. *Id.* at 42.

[78] Just as the Geneva Conventions look to the results of the act (i.e. the injury to sick soldiers, killing civilians, etc.) instead of how the acts were committed (gun vs. knife), the International Group of Experts makes no differentiation between a cyberattack and a conventional use of force. *See* Fourth Geneva Conventions, Aug. 12, 1949, 75 U.N.T.S. 287.

[79] TALLINN MANUAL, *supra* note 12, at 29-36 (Rules Six through Eight consider issues that are not completely germane or essential to the *jus ad bellum* analysis).

[80] *Id.*

[81] *Id.* at 36 (emphasis added).

[82] *Id.*; *see also* U.N. Int'l Law Comm'n, *Responsibility of States for Internationally Wrongful Acts*, art. 22, G.A. Res. 56/83 Annex, U.N. Doc A/RES/56/83 (Dec. 12, 2001).

[83] *See* TALLINN MANUAL, *supra* note 12, at 38. If a state uses the plea of necessity to justify the countermeasures, choosing such a course of action must have been the only way to protect a state's vital interests; *see also* Gabčikovo-Nagymoros Project (Hung. v. Slovak.), 1997 I.C.J. 7, ¶ 55 (Sept. 25, 1997).

interests are as equally protected under this legal approach, but practice and increased incidence rates of cyber-incidents may give rise to challenges.[84] For better or worse, the customary law that governs countermeasures is unchanged for cyberconflict, and thus the Tallinn Manual does not create any legal gaps that were not extant before the advent of cyberwarfare.

2. Rule Ten: Prohibition of Threat or Use of Force

Rule Ten extends the well-settled prohibition[85] on the use of force to cyber operations that constitute a threat or use of force. The prohibitory norm, as established by Article 2, paragraph 4 of the UN Charter, indicates that any use of force is presumptively illegal.[86] Both the prohibition and the presumption on the issue of force could be considered part of customary international law on the use of force. What does this conclusion mean for NATO? By using and extending customary international law to cyberconflict, the Tallinn Manual has disambiguated the nature of cyber operations and sends a clear legal message to nation-states: because a given cyberattack may not rise to the level of an "armed attack" does not mean that it is not illegal.[87] Although the International Group of Experts did not articulate a remedial scheme for a victim state, it would be reasonable to conclude that a state could engage in countermeasures (as defined in Rule 9), or seek remedy in the International Court of Justice.[88] Overall, the Tallinn Manual did treat the issue of the use of force in cyberspace adequately: it clearly and unequivocally stated that a use of force, regardless of the means, is a violation of customary international law,

---

[84] There could be a concern that the plea of necessity may be a difficult justification to prove or comply with because attributing cyberattacks is difficult even under the best of circumstances. *See* David Alexander, *Defense Chief Calls Cyberspace Battlefield of the Future*, REUTERS, Oct. 19, 2012 8:33 PM, *available at* http://www.reuters.com/article/2012/10/20/us-usa-defense-cyber-idUSBRE89J00920121020 ("Identity and attribution on the Internet are not very robust. If you look at kind of the underlying protocols that kind of power the Internet . . . there's no real strong mechanism for identifying where something is coming from"). The potential for a state to act first and evaluate later is high indeed, especially if vital state interests are involved (i.e. the cyberattacks on Estonia that affected vital financial and banking infrastructure). In short, the TALLINN MANUAL should have looked to such an eventuality.

[85] *See* Joseph Miljak, *Forcing Sovereign Conformity: The Comprehensive Anti-Apartheid Act of 1986*, 36 CLEV. ST. L. REV. 261, 284 (1988); John Yoo & Will Trachman, *Less than Bargained for: The Use of Force and the Declining Relevance of the United Nations*, 5 CHI. J. INT'L L. 379 (2005); Jessica Feil, *Cyberwar and Unmanned Aerial Vehicles: Using New Technologies from Espionage to Action*, 45 CASE W. RES. J. INT'L L. 513, 538-39 (2012) (noting in addition to the prohibition, that most non-covert cyber-activities may be a non-armed attack use of force).

[86] TALLINN MANUAL, s*upra* note 12, at 42-43 (Rule 10).

[87] Myriam Dunn Cavelty, *Cyber Allies: Strengths and Weaknesses of NATO's Cyberdefense Posture*, 3 INTERNATIONALE POLITIK: GLOBAL EDITION 11, 14 (Mar. 2011), *available at* http://www.academia.edu/562910/Cyber-Allies_Strengths_and_weaknesses_of_NATOs_cyberdefense_posture.

[88] A victim of a cyberattack could probably bring suit in the ICJ, a situation analogous to the *Nicaragua* judgment. *See generally* Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14 (June 27, 1986).

an excellent outcome for NATO and the legal experts tasked with overseeing a national or institutional response to a cyberattack. Despite this clarification, uncertainties remain in the legal approach to cyber operations under the law of war paradigm.

3. Rule Eleven: Definition of Use of Force

Rule Eleven attempts to define "use of force" as it is defined in Rule Ten, but the rule simply states that a cyber "act" is a use of force when a comparable non-cyber act rises to the use of force threshold. [89] This tautology indicates that Rule Eleven has few concrete guideposts—an unfortunate circumstance for a field of law in dire need of certainty. The Manual notes that the only factor that is certain about the definition of the use of force is that such a definition is uncertain, stating in pertinent part: "There is no authoritative definition of, or criteria for, 'threat' or 'use of force.'"[90] Despite the lack of complete certainty, the International Group of Experts identified that there are some acts that are clearly not uses of force[91] and as a result, the cyber analogs of such acts are also not uses of force. Inversely, there are some acts that are uses of force by virtue of being armed attacks.[92] For the area in between these two extremes, the Tallinn Manual thankfully avoids reverting to the wisdom of Justice Potter of the United States Supreme Court[93] and instead articulates several factors to be weighed when attempting to determine if a given act is a use of force. These factors are: (1) severity, (2) immediacy, (3) directness, (4) invasiveness, (5) measurability of effects, (6) military character, (7) state involvement, and (8) presumptive legality.[94]

While all of these factors are useful for determining whether an act is a use of force, some factors are more pertinent than others. For example, the factors of immediacy and directness (factors that measure the effects of the cyber operation), ultimately hinge on the factor of "measurability of effects." Thus, the two former factors may be ultimately useless in determining whether it is a use of force if there are difficulties in gauging the extent of the "effects". It is equally important to note that other factors, like "military character" are not narrowly tailored to the essence of cyberconflict. While a cyber operation's "military character" may indeed be

[89] The text of Rule Eleven states, "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of the use of force." TALLINN MANUAL, *supra* note 12, at 45.

[90] *Id.* at subsection 2.

[91] The TALLINN MANUAL points to the extensive negotiations over how to characterize a use of force, with a majority of nations determining that mere economic or political pressure lies somewhere below the use of force threshold. *See id.* at 46-47. But just because economic or political pressure does not reach the use of force threshold does not mean that such pressure (or an analogous act) is legal, as such pressure may violate the customary norm against intervention as discussed in Rule 10, subsection 6.

[92] *See id.*

[93] The legendary words, "I know it when I see it" were coined by Supreme Court Justice Stewart Potter in the famous obscenity case *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[94] The TALLINN MANUAL helpfully gives some sample questions that penetrate to the essence of each factor. *See* TALLINN MANUAL, *supra* note 12, at 48-51.

dispositive of state involvement or a use of force, such an association is so elementary that it is almost not even worthy of inclusion, i.e., that a military-style cyber operation is so characteristic of a use of force that the articulation of such a factor is superfluous, and by mere operation of fact, military character is presumed.

The factor of "severity" is the most important consideration when characterizing a cyber operation as a use of force.[95] The Tallinn Manual notes that severity is a de minimis element: acts resulting in physical harm to persons or property will always be a use of force, while minor acts that are little more than irritating will never be a use of force. Cyber operations that fall in the middle, however, are subject to an analysis based on the other factors and other subordinate components of "severity" such as a state's critical interests, scope, intensity, and duration. The Manual itself notes that the element of severity is by far the most important factor to be used when determining if a given act is a use of force.[96]

While there are other factors included in Rule Eleven, many of them are ancillary to an overall determination of whether a cyber operation is a use of force. As a result, a detailed overview of the remaining factors is outside the scope of this analysis.

4. Rule Thirteen: Self-Defence[97] Against Armed Attack

Rule Thirteen contains the most text within the Tallinn Manual relevant to the operations and future planning of NATO cybersecurity policy. As noted above, Article 5 of the Washington Treaty encapsulates the inherent right to individual and collective self-defence as outlined in the UN Charter.[98] Thus, how the Manual treats the scope of the concept of self-defence is fundamentally critical for NATO. The Manual names that the "scale and effects" of a cyber operation are dispositive factors in determining whether an act is indeed an "armed attack."[99] Like other legal standards adopted by the Manual, the "scale and effects" language is also drawn from the wider law of armed conflict.[100] Such an approach removes the process of determining the legal classification of a given attack from the considerations of policy and makes the ultimate determination more empirical. To elaborate, if the only important factors are the scale and effects, then issues like the identity or nature of the attacker or the means of the attack are irrelevant for the purposes of classifying a cyberoperation.[101] Subpart 3 of the rule is incredibly important for the

---

[95] *Id.* ("Subject to a *de minimis* rule, consequences involving physical harm to persons or property will, in and of themselves, qualify as a use of force.").

[96] *Id.* at 48.

[97] A general note on spelling: NATO and the professionals associated with it commonly use "British" spellings of various English words.

[98] U.N. Charter, art. 51, *supra* note 8.

[99] TALLINN MANUAL, *supra* note 12, at 50.

[100] Specifically, it is drawn from the *Nicaragua* judgment of the ICJ. *See Id.* at 47 n.16.

[101] To demonstrate the simple wisdom of such an approach, consider the simple case of homicide. A police officer or prosecutor does not weigh and compare the identity of the suspect, the potential murder weapons, and possible motives in deciding how to classify the *act* (that is, is this a murder, suicide, or accident? The latter two do not require immediate action, while the former does because of the threat to the public). He or she simply looks to whether the victim has been killed. If so, the immediate response is determined: arrest and

purposes of NATO, reiterating the principle that the choice of means is "immaterial to the issue of whether an operation qualifies as an armed attack."[102] Such a viewpoint, however, may not be shared by some experts and officials within the field. But such a stance is not only ignorant of the relevant law, but also displays a disconcerting myopia towards future technological developments. While the Tallinn Manual adopts a more reasoned and, in this author's opinion, a wiser approach, if NATO officials and policymakers are unable to concede in this area, NATO cyber defence policy will be tailored with the assumption that electronic warfare is nothing more than an irritating annoyance instead of a potential force multiplier with nearly unlimited potential for development.

But Rule Thirteen does engender some concerns, because the language of "scale and effects" is not workable. While the legal doctrine is sound, it is unclear how lawyers would implement such a standard in an operational setting. The ICJ opinion that birthed the "scale and effects" standard (Nicaragua v. US) was written long after the commission of the acts that formed the gravamen of Nicaragua's complaint.[103] A lawyer advising a military commander as to the possible responses to a cyber operation cannot ascertain the "effects" as the ICJ could. As an illustration of the problem with the "scale and effects" language, the ICJ unhelpfully stated that a "mere frontier incident" was not an armed attack.[104] But is a "frontier incident" really a "frontier incident?"[105] For the lawyer in the unenviable position of advising a commander using the doctrine of Rule Thirteen, the "scale and effects" can really only be determined with detailed investigation and careful analysis after the fact. So what are the victims of a cyberattack to do in the interim? Perhaps the direness of the circumstances should be the diagnostic factor because "scale and effects" are especially unhelpful in counteracting a cyberattack in progress. [106]

The standard of "scale and effects" and determining whether a qualifying armed attack can trigger the right of self-defence is complicated further by the Group of Experts. While they note that the choice of means is "immaterial," the Group of

---

possible prosecution. An analysis of evidentiary issues and mitigating/aggravating factors does not occur *ex ante* as an initial response, it occurs after necessary measures have been taken (since one justification for arresting a suspected killer is to ensure the killer does not kill again).

[102] *Id.* at 54 n.25 (citing Nuclear Weapons Advisory Opinion ICJ).

[103] The ICJ handed down the *Nicaragua* decision in 1986, but the Sandinista fighting occurred in the late 1970s. *See Nicaragua v. United States*, WIKIPEDIA, http://en.wikipedia.org/wiki/Nicaragua_v._United_States (last visited June 3, 2013).

[104] TALLINN MANUAL, *supra* note 12, at 56.

[105] Wars have started more innocuously than through a major cyber attack. For example, the invasion of Poland in 1939 (which sparked World War II), started as nothing more than German units seizing a border crossing. *See* John Quigley, *Who Admits New Members to the United Nations? Think Twice Before You Answer*, 44 GEO. WASH. INT'L L. REV. 179, 202 n.151 (2012).

[106] The TALLINN MANUAL does provide that a determination of whether a given cyber intrusion is an armed attack should occur *ex ante*, and there is an indication that the foreseeability of harm (people becoming sick after ingesting water from an attacked water plant) can be a factor. *See* TALLINN MANUAL, *supra* note 12, at 57, 60 (subparts 10 and 21).

Experts identified (at least in part) that intent/motive,[107] individual capacity,[108] extent of damage,[109] private/public property,[110] and the status of targeted individuals[111] as pertinent factors in ascertaining whether the right of self-defense can be triggered. As noted above, these additional criterion (or factors), while more useful than a vague or tautological standard, will unnecessarily complicate and hinder quick and prudent legal calculus. To this end, it seems that the drafters lost sight of the practical application of their rules.

E. Criticism of the Tallinn Manual

While there are many reasons that indicate that the Tallinn Manual is a well-drafted document worthy of international recognition, there are some concerns with the Manual's contents that will confound legal scholars and policymakers. First, the manual is non-empirical. Unlike a common law court opinion, the Tallinn Manual only lists the conclusions of the group of experts. To analogize, it is as if the Manual is a collection of ninety-five case holdings with explanations that range from barely adequate to exceedingly sparse. There is no comparison of conflicting viewpoints, no survey of the evidence—it is as if the Manual exists in some vacuous ephemera aloof to policy considerations, current trends, and past events.

Second, when the Manual does tread upon contentious issues, it barely resolves them. Brief synopses of the opinions of the group of experts are included, but such inclusions are functionally worthless for scholars and researchers. The Manual speaks in terms of "some," "many," or "all" when referencing the Group of Experts' opinions on various issues. The substance of their discussions, a record of the vote or even the identities of the dissenters could have exponentially increased the usefulness of the Manual for those paying attention to the development of law in this novel area. If the Manual disclosed which experts came to which specific conclusions, it could have facilitated analysis in determining which nations and organizations condoned or supported the views of their experts, thus enhancing the predictability of the Manual's implementation. In addition, including such information would aid in tracking how pervasively the Manual is being adopted by governments and other entities, or aid in identifying potential "differences in opinion" among the NATO allies and their professionals.

Third, the Manual reads as if unsure of its audience. Rule Thirteen meanders especially, leaving the reader with as many questions as a first-year law student leaving a complex contracts class. In this regard, the Manual seems to be less of a Manual and more of a treatise, a voluminous work that sets out roughly crafted rules that need revision or refinement. It will be difficult for any lawyer to use the Manual as it is for anything more than a foundational, doctrinal document.

But the Manual also divorces its doctrine from theory, as well as practical considerations, and perhaps that is its greatest fault. If theory roughly equates to the

---

[107] *Id.* at 57 (subpart 11).

[108] *Id.* at 59 (subpart 17).

[109] *Id.* (subpart 19).

[110] *Id.*

[111] *Id.*

goal that the law seeks to achieve,[112] then the Group of Experts should have made rules that would make it easier for IT personnel, security professionals and lawyers to apply the rules in exigent circumstances. In short, the Manual should have articulated some guiding principles for practitioners based on the international law. Instead, the Rules embody customary international law (except where otherwise noted),[113] but therein lies the problem. Customary international law remains decidedly unclear (or, at the very least, in flux) and, to simply revert to these old international norms is to almost state that there is no useful norm at all, like there is nothing different or unique about the situations posed by cyber warfare.[114] The very reason the Tallinn Manual should exist is to guide governments and organizations like NATO in a brave, new world of warfare. Thus, if there ever was a chance to make the law from scratch, and to truly wax poetic on what that law should look like, drafting the Tallinn Manual was that chance. But the Manual is hesitant and conservative. For example, the question of whether a cyberattack that crashes a stock exchange should constitute an armed attack went unresolved.[115] Simply put, the Manual could have tackled the more thorny legal issues more earnestly.

IV. CONCLUSION

The Tallinn Manual promises to be a seminal document in the "law of cyberwarfare." While the Manual has myriad issues, it stands as a solid theoretical statement of the law of armed conflict in the 21st century. Beyond its own strengths, the Manual should form the basis of a new experiment in the field of international humanitarian law and as such could gain much by using the labors of the International Group of Experts. The Manual can be regarded as a conservative, well-reasoned (albeit imperfect) statement of what the law should be in this exciting new field.

---

[112] Or in other words, the goal of theory is to generate solutions to legal problems. *See* Joseph William Singer, *The Player and the Cards: Nihilism and Legal Theory*, 94 YALE L.J. 1, 61 (1984) (stating that the goal of theory is to "provide answers").

[113] TALLINN MANUAL, *supra* note 12, at 6.

[114] *See* Timothy Meyer, *Codifying Custom*, 160 U. PA. L. REV. 995, 1002-03 (2012) ("Customary international law, as the commonly cited definition goes, 'results from a general and consistent state practice' done out of 'a sense of legal obligation.' This definition, although easily stated, turns out to be terribly difficult to apply."). *See generally* David H. Moore, *The President's Unconstitutional Treatymaking*, 59 UCLA L. REV. 598 (2012) (noting, in parts, that the extent to which interim treaty obligations attach on the United States is unclear, but is unconstitutional); Frederic Sourgens, *Law's Laboratory: Developing International Law on Investment Protection as Common Law*, 34 NW. J. INT'L L. & BUS. 181 (2014) (arguing that investor-state relations are an example of new customary international law).

[115] A brief discussion of a Stock Exchange scenario appeared in a draft of the TALLINN MANUAL. TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Int'l Group of Experts, Working Paper, 2013), *available at* http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf). On page 53 (subpart 9) of the manuscript, Rule Thirteen was later removed from the document (at least, according to this author's research). In any event, it is probable that the International Group of Experts was unwilling to commit to any one approach. *See id.*

If the efficacy of an alliance is measured by how well it keeps the peace among its constituents, NATO is indeed successful. Outside of a few terrorist attacks, the members of NATO have remained more or less protected and secure for the greater part of the Alliance's history. Yet prevention requires prospection. NATO must be cognizant of not only current trends but also future possibilities. The Tallinn Manual is a necessary first step in the development of NATO's capabilities in cyberwarfare. While not a panacea, the Manual has the capability to align itself with NATO's preventative outlook by providing the Alliance with the tools to make cyberconflict less anarchic and less uncertain. If nation-states operate in cyberspace like they did prior to the promulgation of the major international human rights and international humanitarian law treaties, commerce, communication, diplomacy and political cooperation will undoubtedly suffer from the incursions of unbridled cyberattacks. While some "rules" may be obeyed in the interim, the protocols for cyberconflict may be abandoned when necessary or convenient.

While it would be incredible to argue that information warfare, left legally unchecked, could wreak as much havoc as its kinetic cousins, the wise may nevertheless be concerned. Just because the harm to be prevented is not as invidious as its kin does little to convince the vigilant that action is any less necessary. Undoubtedly, the outlandishness of the hypothetical cyber-bogeyman disarms even a well-reasoned analysis—and may be responsible for the academy's overall lack of interest in the Manual and cyber warfare.[116]

In sum, the Tallinn Manual represents a solid effort to state the current law as it applies to current situations. Given the overall dearth of bright line rules and practical principles, the Manual is more of a treatise, but is nevertheless a bold step forward. In considering NATO's history, encounters with cyberconflict, and the overall international political attitudes towards cyberconflict, the Tallinn Manual's rules and commentaries may soon need revision. In any case, the generals, lawyers, and politicians that make up NATO and lead its constituent countries will need additional guidance in this new era of cyber warfare.

[116] A search of the SSRN database using the words "TALLINN MANUAL" returned only thirteen papers mentioning the Manual. *SSRN eLibrary Database Search Results*, SSRN, http://papers.ssrn.com/sol3/results.cfm (last visited Aug. 7, 2014).