National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

REAL PROBLEMS IN THE VIRTUAL WORLD: INTERNATIONAL LAW PRIORITIES REGARDING CYBER-CONFLICT

LCol D.W. Brown

JCSP 42

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 42

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

REAL PROBLEMS IN THE VIRTUAL WORLD: INTERNATIONAL LAW PRIORITIES REGARDING CYBER-CONFLICT

LCol D.W. Brown

Word Count: 4810

Compte de mots: 4810

Here's the problem – it's 1946 in cyber.

— James Mulvenon, *The New Cyber Arms Race*

INTRODUCTION

Cyberspace, a globally-interconnected information infrastructure, provides a new field of operations where belligerents can prey on state governments, private industries, and domestic infrastructure irrespective of their location on the globe using the victim's own information and communications technology (ICT) against itself. These 'cyber-attacks' can be carried out anonymously and have the potential to cause large-scale destruction in both the cyberspace and the physical world.[1] In less than a decade there have already been four well recognized acts of cyber-conflict to emphasize the growing risks of cyber-attack: the 2007 attacks on Estonia, the 2007 attacks on Syrian air defence, the 2008 attacks during the Russo-Georgian War, and the 2010 Stuxnet attack on Iranian nuclear program.[2] These four examples show that contemporary armed conflict now includes a cyber dimension and this new dimension is being integrated with other strategies of warfare: kinetic, political, and economic.[3] It should be no surprise that cyberspace has become important to military operations as ICTs have been steadily adopted by militaries to improve their combat effectiveness and efficiency.[4]

---

[1] Christopher D DeLuca, "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors." Pace International Law Review Online Companion 3, no. 9 (January 1, 2013): http://digitalcommons.pace.edu/pilronline/34, 279, 282; Michael N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2013). 24; Wolff Heintschel von Heinegg, 'The Tallinn Manual and International Cyber Security Law', in *Yearbook of International Humanitarian Law Volume 15,* ed. T.D. Gill et al. (The Hague, The Netherlands: T.M.C. Asser Press, 2013), 5.

[2] Randall R. Dipert, 'Other-than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy', *Journal of Military Ethics* 12, no. 1 (April 2013), doi:10.1080/15027570.2013.785126; 40.

[3] Vijay M. Padmanabhan, "Cyber Warriors and the Jus in Bello." *International Law Studies* 89 (2013): 289; Massimo Durante, "Violence, Just Cyber War and Information," ed. Ludovica Glorioso and Anna-Maria Osula, in Workshop on Ethics of Cyber Conflict (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, n.d.), https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf, 59.

[4] von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 8.

Cyber-conflict changes the nature of conflict. Cyber-attacks have the potential to cause large-scale economic and sociological disruption without the expected physical damage of a kinetic armed conflict. Cyber-conflict is innately transnational and cyber-attacks can be launched by relatively small groups, or a single individual. These characteristics of cyber-warfare are very different from traditional warfare where the rules of war are based on physical destruction, geographical boundaries, and the armed forces of a sovereign state.[5]

Cyber-security has become a prominent feature on the national security agenda of many states due to the potential devastating impacts of a cyber-attack and the proliferation of cyber-warfare technology. The Australian government named 'malicious cyber activity' as one of its key national security risks in the 2013 Australian National Security Strategy.[6] President Obama announced in the 2011 International Strategy for Cyberspace that the United States has,

> …the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[7]

Despite state efforts, cyber-conflict is a worldwide concern that must be dealt with internationally.[8]

While the international community has identified cyber-conflict as a growing concern that requires attention, the bulk of the legal analysis completed thus far has been done by private

---

[5] Schmitt, Michael N. "Classification of Cyber Conflict." *International Law Studies* 89 (2013): 234; United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, (New York: United Nations, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172, 6.

[6] Nicholas G. Evans et al., *Cybersecurity: Mapping the Ethical Terrain* (Australian National University, Acton: National Security College, 2014), 17; Bradley Raboin, "Corresponding Evolution: International Law and the Emergence of Cyber Warfare." *Journal of the National Association of Administrative Law Judiciary* 31, no. 2 (October 15, 2011): http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5, 629.

[7] United States of America. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: United States of America, 2011.

[8] Raboin, "Corresponding Evolution" … 632.

business, academics, militaries, and state governments.[9] There have been only three international groups that have addressed cyber-warfare over the past few years:[10] the 2001 European Union Council Convention on Cybercrime,[11] the 2002 and 2007 North Atlantic Treaty Organization (NATO) cyber-warfare summits,[12] and the unofficial 2010 United Nations (UN) cyber-warfare proliferation meeting.

In order for the international legal community to accomplish the necessary analysis and then create legal systems to effectively regulate the waging of cyber-war, it is necessary to prioritize the areas that need to be addressed. The most important and urgent area of cyber-concern that the international legal community should cooperatively focus on is cyber-crime. This paper will analyze five of the most pressing and significant legal challenges to effectively managing cyber-conflict - attribution, legal definition, distinction, malicious non-state actors, and crime - and show that the global community would most benefit from international legal attention towards crime. Before being the analysis, it is first necessary to provide some background information regarding international law pertaining to cyber-warfare as well as the *Tallinn Manual on the International Law Applicable to Cyber Warfare.*

BACKGROUND

International Law

There are two bodies of international law that regulate war: j*us ad bellum* and *jus in bello*. *Jus ad bellum* controls when a state may resort to force based largely on the 1919

[9] Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law', *Texas Law Review* 88, no. 7 (June 2010), 1571, 1584.

[10] Raboin, "Corresponding Evolution"…633-6.

[11] The EU Council Convention on Cybercrime was signed by 41 states, including the US and Canada. However, the convention does not apply to cyber-warfare.

[12] As a result of these summits, NATO stood up the Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia to focus on the defence against advanced cyber-attacks.

Covenant of the League of Nations, the 1928 Kellogg-Briand Pact, and the United Nations Charter. *Jus in bello* regulates the activities during an armed conflict and is often referred to as the Laws of Armed Conflict (LOAC), Laws of War, or International Humanitarian Law (IHL). *Jus in bello* references the Geneva Conventions and customary law dealing with international armed conflict, plus a limited body of law dealing with non-international armed conflict. IHL aims to lessen war suffering by protecting persons not contributing to hostilities and by limiting the means and methods of conflict.[13] For the purposes of this paper, the use of IHL will be considered synonymous with LOAC or Laws of War.

There are currently no cyber-warfare specific treaty provisions and, due to the secrecy surrounding the activity of most states in the cyber-domain, there are few publicly available expressions of *opinio juris*. This inhibits efforts to determine if any cyber-specific customary international law norm exists.[14]

Over the past two decades, there had been debate among academic and policy communities regarding the applicability of international law to cyberspace.[15] One approach was for the establishment of *lex specialis*, an international treaty regulating the use of cyberspace. This alternative was initially suggested to the United Nations by Russia and China in 2004 and

---

[13] Bill Boothby, "Law, Ethics and Cyber Warfare," ed. Ludovica Glorioso and Anna-Maria Osula, in Workshop on Ethics of Cyber Conflict (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf.17; Laurie R. Blank, "International Law and Cyber Threats from Non-State Actors." *International Law Studies* 89 (2013): 407-8, 410, 420; Diakonia International Humanitarian Law Resource Centre. "Basic Principles of IHL." October 30, 2013. Accessed April 20, 2016. https://www.diakonia.se/en/ihl/the-law/international-humanitarian-law-1/introduction-to-ihl/principles-of-international-law/.

[14] Schmitt, Tallinn Manual… 19; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016; Boothby, "Law, Ethics and Cyber Warfare," … 23.

[15] Scott J Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge: Cambridge University Press, 2014). 264.

was supported by member states of the Shanghai Cooperation Organization and Brazil. Support for such a treaty could not be found in the United Nations Security Council.[16]

There is now generally wide-spread agreement that international laws do apply to cyberspace and the debate has begun to turn to how the law should apply, even Russia and China have recently begun to support this position.[17] There are four major references worth noting that helped to convince the international community to the applicability of international law to cyberspace:

- Protocol I, Article 36. This article says that states must ensure that any new weapons comply with the rules of IHL. This article allows for the continued applicability of IHL as the means and methods of war evolve over time.[18]
- International Court of Justice's Advisory Opinion on the Legality of Nuclear Weapons. This advisory opinion stated that *jus ad bellum* applies ''to any use of force, regardless of the weapons employed'' and that the conduct of warfare is ruled by IHL at the start of any armed conflict.[19]

---

[16] United States, United Kingdom, and France would not support the suggestion. Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law' … 1588.

[17] Michael N. Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack', *International Review of the Red Cross* 96, no. 893 (March 2014), doi:10.1017/s1816383114000381. 206; von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 9-10; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016; International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, (Geneva: International Committee of the Red Cross, 2015): 39, 44. https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

[18] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, June 8, 1977. art. 36; Spencer Kimball, 'NATO Moves to Apply Armed Conflict Law to Cyber Warfare', *Deutsche Welle* (Deutsche Welle), July 2, 2014, http://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359; 'What Limits Does the Law of War Impose on Cyber Attacks?', International Committee of the Red Cross, July 1, 2013, accessed March 30, 2016, https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

[19] International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*. Report 226, 1996; von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 9-10; Schmitt, Tallinn Manual… 17; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

- Tallinn Manual on the International Law Applicable to Cyber Warfare.[20] Importance of this document is further described in the next section of this paper.
- Reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. In both the 2013 and 2015 reports, the Group of Governmental Experts (GGE) stated that,

> International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT [information and communications technology] environment.[21]

These reports have gone on to stress the importance of the principles of humanity, necessity, proportionality, and distinction.[22]

While the international community predominantly agrees that international law applies to cyberspace, there are still many shortcomings when it comes to the establishment of international norms surrounding conflict in cyberspace.

Tallinn Manual

In 2009, NATO sponsored the first serious effort to better under how existing international law applies to cyber-warfare. At this time there was considerable international debate regarding the applicability of IHL to cyber-warfare. Cyber-activities were being conducted without a clear legal framework and there were claims that, during an armed conflict, cyberspace was not subject existing international law conflict.[23] Through the NATO Cooperative

---

[20] Schmitt, *Tallinn Manual*

[21] United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, (New York: United Nations, 2013), http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156. 8; ICRC, *International Humanitarian Law and the Challenges* ... 39.

[22] UN, 205 Report by GGE ... 3.

[23] Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016; Michael N Schmitt, 'International Law and Cyberwar: A Response to the Ethics of Cyberweapons', *Ethics & International Affairs*, February 10, 2014, http://www.ethicsandinternationalaffairs.org/2014/international-law-and-

Cyber Defence Centre of Excellence (CCD COE), an international military organization charged with enhancing cyber defence cooperation among NATO member nations, a group of 20 experts were invited to Tallinn, Estonia, to produce a non-binding legal manual applying existing IHL to cyber-warfare. This 'International Group of Experts,' selected by the project's director, Michael Schmitt,[24] laboured for more than three years to eventually produce the *Tallinn Manual on the International Law Applicable to Cyber Warfare (*Tallinn Manual*)*.[25]

The International Group of Experts approach used by Schmitt to produce the Tallinn Manual was consistent with previous approaches to the application of international law towards new technologies. The concept of bringing legal experts together to 'study, clarify, and develop' international law goes as far back as 1873, when the International Law Association was formed, and was institutionalized by the United Nations in 1947 with the establishment of the International Law Commission. The process of writing the Tallinn Manual resembles the process used for a number of recent projects: San Remo Manual on International Law Applicable to Armed Conflicts at Sea and the Manual on International Law Applicable to Air and Missile Warfare[26]

---

cyberwar-a-response-to-the-ethics-of-cyberweapons/; Kimball, 'NATO Moves to Apply Armed Conflict Law to Cyber Warfare'; 'What Limits Does the Law of War Impose on Cyber Attacks?', ICRC.

[24] Michael N. Schmitt is an international law scholar specializing in international humanitarian law and use of force issues. He is the Chairman of the Stockton Center for the Study of International Law at the United States Naval War College. Schmitt has participated in multiple international expert working groups, including: Manual on the International Law of Air and Missile Warfare, Civilians in Hostilities, and Characterization of Conflict. Schmitt was an intelligence officer and judge advocate during his 20 years with the United States Air Force.

[25] Schmitt, *Tallinn Manual…* 1-11; Schmitt, 'International Law and Cyberwar'; Oliver Kessler and Wouter Werner, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare', *Leiden Journal of International Law* 26, no. 04 (November 8, 2013), doi:10.1017/s0922156513000411. 805.

[26] Schmitt, *Tallinn Manual…*16; von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 12; Charles J. Dunlap, 'Some Reactions on the Intersection of Law and Ethics in Cyber War', *Air & Space Power Journal* 27, no. 1 (2013), 24; Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 793.

The Tallinn Manual was restricted to the restatement and analysis of *lex lata* (existing international law) of *jus ad bellum* and *jus in bello*.[27] The International Group of Experts; that eventually included scholars, lawyers, technical experts, and cyber practitioners; were in complete agreement that *lex lata* fully applies to cyberspace during war. However the group did also identify a variety of situations when the nature of cyberspace would require legal interpretation efforts to fit the law into the cyber realm.[28] The nearly 300 page manual includes 94 restatements of *lex lata* (referred to as 'laws' within the manual) and more extensive analysis (referred to as 'commentary') for each rule, including explanation of any differences of opinion between the experts on each law.[29]

There have been a number of criticisms of the overall Tallinn Manual project. The most prominent criticism is that the International Group of Experts came principally from Western nations and therefore the manual reflects a geographical bias towards the West, and NATO countries in particular.[30] There was also criticism that the simple effort of analyzing cyber activities through a lens of cyber-conflict militarizes the very nature of cyber-security discourse.[31] The most important success of the Tallinn Manual has been that it has served as a fuel for serious debate surrounding the acceptable use of cyber-activities in armed conflict.[32]

---

[27] von Heinegg, 'The Tallinn Manual and International Cyber Security … 4, 12.

[28] Schmitt, *Tallinn Manual*... 1-11; Schmitt, 'International Law and Cyberwar'; Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 805; von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 4; Kimball, 'NATO Moves to Apply Armed Conflict Law to Cyber Warfare.'

[29] Schmitt, *Tallinn Manual*... Adam Klein, 'Tallinn 2.0 and a Chinese View on the Tallinn Process', *Lawfare*, January 14, 2016, https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process; Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 807.

[30] von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 11; Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 805; Klein, 'Tallinn 2.0 and a Chinese View on the Tallinn Process'.

[31] Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 809.

[32] von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 14; 'What Limits Does the Law of War Impose on Cyber Attacks?', ICRC.

The NATO CCD COE as already sponsored a follow-up project to the Tallinn Manual, dubbed 'Tallinn 2.0'. This new project further extends the scope of the Tallinn Manual to see how international law applies to malicious cyber-activities below the level of armed attacks and use of force. By enlarging the scope of the project, there is an expectation that the manual will be more influential as it will address activities that are more commonly found in cyberspace. Another improvement of the Tallinn 2.0 effort is that the International Group of Experts now includes representation from Russia, China, and Israel. Tallinn 2.0 is expected to be completed in 2016.[33]

CHALLENGES

Attribution

The most commonly identified cyber-warfare problem regarding IHL is that of attribution as it is more challenging in cyberspace, due to global connectivity of ICT networks, to discern the perpetrator of a cyber-attack. In cyberspace, the identity of the offending party can be disguised by distributing both the cyber-attackers and the actual cyber-attack across platforms and jurisdictions. The attacker can use these deceptive manoeuvres to not only conceal their own identity but also to falsely incriminate a third-party or simply create a situation of plausible deniability.[34]

---

[33] Schmitt, 'International Law and Cyberwar'; Klein, 'Tallinn 2.0 and a Chinese View on the Tallinn Process'; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[34] Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations…* 146; Neil C. Rowe, 'Ethics of Cyberwar Attacks', in Cyber warfare and cyber terrorism, by Lech Janczewski and Andrew Colarik (n.p.: Information Science Reference, 2007); Michael J Glennon, "The Road Ahead: Gaps, Leaks and Drips." *International Law Studies* 89 (2013): 382; Raboin, "Corresponding Evolution" …640. Randall R. Dipert, 'The Ethics of Cyberwarfare', *Journal of Military Ethics* 9, no. 4 (December 2010), doi:10.1080/15027570.2010.536404. 385; UN, 2013 *Report of the GGE* … 6.

The ability of a victim state to attribute an attack to the perpetrator is a foundational requirement of existing laws of war that regulates armed conflict. It is so important that *just in bello* requires states to identify themselves when attacking another state.[35] Attribution is necessary for the victim state of a cyber-attack to figure out their right of reprisal and self-defence. A state has very different options available to them, under *jus ad bellum*, if the offending party is a state, a non-state actor, or simply an individual. Also, the identity of one's foe is required so that the victim state can select an appropriate response that will not cause undue collateral damage. If the perpetrator cannot be identified, a number of principles and laws become meaningless: protection of non-combatants, principle of distinction, proportionality, prohibition of aggression, law of neutrality, and the responsibility of command.[36]

Chapter 1, section 2 (State Responsibility) of the Tallinn Manual speaks most directly to the attribution problem[37] and Rules 7 and 8 attempt to address some specific attribution concerns. Rule 7 focuses on cyber-attacks launched from a government infrastructure,

> The mere fact that a cyber-operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation.[38]

---

[35] Glennon, "The Road Ahead: Gaps, Leaks and Drips." … 380; Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations:…* 291.

[36] Raboin, "Corresponding Evolution" … 640. Rowe, 'Ethics of Cyberwar Attacks'… 382; Glennon, "The Road Ahead: Gaps, Leaks and Drips." ... 380; Blank, "International Law and Cyber Threats from Non-State Actors." ... 426; Herbert Lin, 'Cyber Conflict and International Humanitarian Law', *International Review of the Red Cross* 94, no. 886 (June 2012), doi:10.1017/s1816383112000811. 521.

[37] Schmitt, Tallinn Manual… 35-40.

[38] Ibid.

Rule 8 looks at cyber-attacks traversing through a state, "The fact that a cyber-operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State."[39]

There has been some discussion on what degree of certainty is required to identify the perpetrator before being legally permitted to respond with lethal or non-lethal force. Using 'compound methods of attribution,' where a variety of intelligence and technical investigative methods combined with circumstantial evidence, the perpetrator could be determined to a 'beyond a reasonable doubt' standard.[40] Of course this approach would delay prompt attribution and there runs a risk of false attribution.

Ultimately, attribution is a technical problem and not one that lawyers can remedy.[41] We will now investigate how technically difficult attribution is.

The challenge of technical attribution is continually affirmed in the vast majority of literature on the subject. While it is certainly more difficult to attribute a cyber-attack than an attack in the physical world, difficult should not be misinterpreted as impossible. It is true that technical attribution is resource-intensive, can rarely be accomplished in real-time, and identification of the perpetrating computer does not determine the responsible state, or

---

[39] Ibid..

[40] Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations*… 291; Raboin, "Corresponding Evolution"… 642-6. Edward T. Barrett, "The Applicability of the Just War Tradition to Military Cyber Operations," ed. Ludovica Glorioso and Anna-Maria Osula, in Workshop on Ethics of Cyber Conflict (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf, 28; Dipert, 'Other-than-Internet (OTI) Cyberwarfare' … 38.

[41] William Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." International Law Studies 89 (2013): 189; Dunlap, 'Some Reactions on the Intersection of Law and Ethics in Cyber War'… 24.

individual. At the time that the Tallinn Manual was written, there was only a limited technical attribution capability resident in any state.[42]

Great strides have been made in technical attribution over the past five years. Using technical forensics, analysts are able to learn much about the techniques, procedures, and behaviours of cyber-attackers. These clues allow analysts to identify the signature of particular cyber-actors and these signatures aid in attribution efforts.[43] While they are unlikely to admit it, so as not to compromise intelligence sources or admit their own cyber capabilities, states with advanced cyber programs are now generally able to precisely determine the perpetrator of a cyber-attack.[44]

In this section we have learned three important aspects of the attribution problem: attribution is at the heart of effective legal regulation of war, the attribution problem is technical in nature, and technical attribution is difficult but not as impracticable as initially thought.[45]

Legal definition

IHL, and other international treaties and agreements pertaining to conflict, were designed to address conflicts waged in the physical domain with kinetic weapons. As a result, these legal instruments use language that is not easily adapted to cyber-warfare. What further complicates matters is that key terms within the UN Charter were never definitively defined to begin with and the Charter is inconsistent with itself in certain areas. Hence, this 'definition problem' has

---

[42] Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility', *Melbourne Journal of International Law* 14 (2013). 502-3; Jack Goldsmith, "How Cyber Changes the Laws of War." *European Journal of International Law* 24, no. 1 (February 1, 2013): 131-2; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[43] Margulies, 'Sovereignty and Cyber Attacks' … 504.

[44] Alexander Moens, *Cybersecurity Challenges for Canada and the United States*, (Vancouver, BC: Fraser Institute, 2015), 6; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[45] Dipert, 'Other-than-Internet (OTI) Cyberwarfare' … 38.

troubled the security community for many years and now it increases confusion over how these international instruments apply to the cyber-warfare.[46]

Often referred to as the 'ontological problem,' there is a legal problem with the non-material nature of objects in cyberspace. Protocol I outlines numerous protections to objects but all examples refer to physical objects and not entities that are virtual (data, activities, processes, etc.).[47] If data is considered as an object, then cyber-activities that change or delete data would be considered as attacks, and if those attacks were hostile to civilian data they would be considered unlawful.[48] This issue is covered in the Tallinn Manual in two places: chapter IV, section 4, (Attacks against Objects) and chapter V, section 7, rule 81 (Protections of Objects Indispensable to Survival). The commentary for these rules notes that most of the International Group of Experts were averse to consider data as an object, as *lex lata*.[49] They were largely swayed by the ICRC's Commentary on Article 52 (the prohibition on attacking civilian objects) that "in both English and French the word (object) means something that is visible and tangible."[50] Data has neither of these properties. Despite this *lex lata* interpretation that data is not an object, it is likely that *lex ferenda* will reverse this perspective in order to ensure the IHL remains valid.[51]

---

[46] Dunlap, 'Some Reactions on the Intersection of Law and Ethics in Cyber War'… 23; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 36; Lin, 'Cyber Conflict and International Humanitarian Law'… 524; Corinne J.N. Cath, Ludovica Glorioso, and Maria Rosaria Taddeo, *NATO CCD COE Workshop on 'Ethics and Policies for Cyber Warfare' (Magdalen College, Oxford)*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/sites/default/files/multimedia/pdf/report_workshop_on_ethics_publication.pdf, 8.

[47] Protocol I; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 37; Dipert, 'The Ethics of Cyberwarfare'… 399-400.

[48] Schmitt, 'Rewired Warfare' … 200.

[49] Schmitt, *Tallinn Manual*... 124-139; Schmitt, 'Rewired' … 201; Noam Lubell, "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?" *International Law Studies* 89 (2013): 267.

[50] "Commentary of 1987 General Protection of Civilian Objects," International Committee of the Red Cross, 1987, accessed May 6, 2016, https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5F27276CE1BBB79DC12563CD00434969; Schmitt, 'Rewired Warfare' … 200.

[51] Schmitt, 'Rewired Warfare' … 204.

The second problem of definition deals with a longstanding confusion of when IHL begins to apply in a conflict as Article 2(4) of the United Nations Charter uses terms of "armed attack" and "use of force" that have never been adequately defined. The few interpretations that do exist deal with traditional kinetic weapons in the physical world.[52] As a result, there is increased debate within the international legal community regarding the interpretation of the term "attack" within cyberspace. There are only two areas of general consensus thus far: state cyber-activities that result in the injury to persons or physical damage to objects are considered attacks and not all cyber-activities affecting a civilian population are consider unlawful.[53]

The Tallinn Manual experts acknowledge that the term 'attacks' should not be limited to injurious or physically damaging cyber-activities but this was a *lex ferenda* opinion and not based on *lex lata*.[54] One of the concerns is if cyber-activities not causing injury or damage but potentially leading to other disastrous effects (i.e. the disruption of economic systems) are not considered attacks then far more non-traditional targets become accessible.[55] Due to the seeming lack of effective *lex lata*, various criterion are being considered to determine if a cyber-attack constitutes an armed attack: a 'functionality test' related to the function of the targeted object, the 'effects-based approach' that compares the effects of a cyber-attack to those caused by conventional means, and the 'Schmitt analysis' that looks at seven factors of permissibility.[56]

---

[52] Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016; Durante, "Violence, Just Cyber War and Information,"… 60-61; Lubell, "Lawful Targets in Cyber Operations" … 275; DeLuca, "The Need for International Laws of War… 294. http://digitalcommons.pace.edu/pilronline/34/; Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." … 184; Tom Gjelten. "Extending the Law of War to Cyberspace." September 22, 2010. Accessed April 23, 2016. http://www.npr.org/templates/story/story.php?storyId=130023318; Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 807.

[53] Schmitt, 'International Law and Cyberwar'.

[54] Schmitt, *Tallinn Manual*... 42-60.

[55] Lubell, "Lawful Targets in Cyber Operations" ... 260; Kimball, 'NATO Moves to Apply Armed Conflict Law to Cyber Warfare'.

[56] Schmitt, 'Rewired Warfare' … 191-2; Lianne J.M. Boer, '"Restating the Law 'As It Is'": On the Tallinn Manual and the Use of Force in Cyberspace', *Amsterdam Law Forum* 5, no. 3 (2013). 10; Blank, "International Law

The virtualization of IHL terminology is proving to be a slow and complicated process. Even so, the problem of uncertain legal terms is not limited to the cyber-warfare; it is prevalent throughout international law.[57]

Distinction

In armed combat, the principle of distinction requires that lawful targets are identified as a precondition to the use of force. A legitimate attack must be directed at a legitimate target: soldiers, members of a structured armed force, civilians directly contributing to the conflict, or military objectives. This principle of distinction is one of the fundamentals of IHL and therefore should then remain valid in any conflict.[58] However, conflict in cyberspace presents challenges to the distinction principle. In cyber-warfare, civilians and civilian objects are ubiquitous on the battlefield and our ability to discern military from civilian is complicated.[59]

The distinction problem for civilians in cyberspace pertains to the status of civilians who participate in aggression. Similar to the ongoing debate over the status and use of private military and security contractors (PMSCs) in conflict zones, there are many civilians involved in military cyber-activities and the existing IHL rules do not yet sufficiently account for their participation in conflict.[60] Rule 35 (Civilian Direct Participants in Hostilities) is the primary attempt of the

---

and Cyber Threats from Non-State Actors." ... 415; Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations*... 288-289; Rowe, 'Ethics of Cyberwar Attacks'… 382; Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[57] Randall R. Dipert, "Distinctive Ethical Issues of Cyberwarfare," ed. Ludovica Glorioso and Anna-Maria Osula, in Workshop on Ethics of Cyber Conflict (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf, 35; Raboin, "Corresponding Evolution" … 655.

[58] The principle of distinction can be found in Protocol I (Article 28, 48, 51, 58, and 85), the Rome Statute, and customary international law as upheld by the International Criminal Tribunal for the former Yugoslavia in the Tadi case. Blank,"International Law and Cyber Threats from Non-State Actors." ... 426-7.

[59] Lin, 'Cyber Conflict and International Humanitarian Law'… 521; Lubell, "Lawful Targets in Cyber Operations" … 253; Blank, "International Law and Cyber Threats from Non-State Actors." ...427-8.

[60] Barrett, "The Applicability of the Just War Tradition to Military Cyber Operations," … 32.

Tallinn Manual to clarify the *lex lata* but other rules also deal with this phenomenon.[61] Currently civilians who "directly participate in the hostilities" lose their protection from attack only while they participate in the cyber-conflict. Additionally, civilians who directly participate in hostile cyber-activities do not enjoy the 'belligerent immunity' of soldiers; they may be prosecuted by a state for violations of domestic law.[62] The International Committee of the Red Cross (ICRC) supports a strict interpretation of the existing *lex lata* in that civilians immediately regain their protected status once they have completed any specific hostile cyber-acts. The Tallinn experts disagree with this viewpoint as civilians performing hostile cyber-acts commonly have the intent to commit future acts.[63] Questions continue regarding the potential status of civilian contractors designing cyber-weapons, criminal organizations hired by a state to launch cyber-attacks, 'hacktivists' encouraged by a state take cyber-action, or civilian cyber-security experts that defend dual-use cyber-infrastructure from incoming attacks.[64]

The other distinction concern in cyberspace is the combined civilian and military use of cyber-infrastructure and how to determine lawful military objectives.[65] It is estimated that up to 95 percent of U.S. military and intelligence communications traverse civilian networks such as submarine fibre-optic cables, communication satellites, and general ICT hardware and software.[66] In Canada, with the 2011 establishment of Shared Services Canada,[67] the majority of

---

[61] Schmitt, *Tallinn Manual*... 118-121.

[62] Schmitt, 'International Law and Cyberwar'; Dunlap, 'Some Reactions on the Intersection of Law and Ethics in Cyber War'… 28; Blank, "International Law and Cyber Threats from Non-State Actors." ... 429-30.

[63] Kessler and Werner, 'Expertise, Uncertainty, and International Law'… 807; Barrett, "The Applicability of the Just War Tradition to Military Cyber Operations," … 2.

[64] Padmanabhan, "Cyber Warriors and the Jus in Bello."... 293.

[65] Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations*... 300; Lubell, "Lawful Targets in Cyber Operations" … 256.

[66] Gjelten, "Extending the Law of War to Cyberspace."; Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law'… 1595.

[67] Shared Services Canada Act, S.C. 2012, c. 19, s. 711, 2012, (Government of Canada).

military ICT services are being merged into a common government system.[68] This combined use of infrastructure is referred to as the 'dual-use' phenomenon and is so prevalent worldwide that it is most often not possible to distinguish between civilian and purely military cyber-infrastructures.[69] In traditional kinetic targeting, dual-use infrastructure could be considered a lawful military objective based on proportionality (i.e. the military outcome was worth the potential collateral damage). Application of this traditional kinetic approach into cyberspace could lead to the identification of the majority of cyber-infrastructure as military objectives and therefore not be protected against cyber or kinetic attack.[70] There are a number of opponents to this line of reasoning that believe both civilian and dual-use cyber-infrastructure should never be considered as legitimate military targets.[71] Of course, this alternative argument would encourage belligerents to shield their ICT capabilities behind the protection of dual-use cyber-infrastructure.

Both of these distinction issues, status of civilian belligerents and dual-use cyber-infrastructure, require more than a simple re-interpretation of existing IHL. The principle of cyber-distinction requires further debate among the international community to gain consensus followed by the establishment of new rules.

Malicious Non-State Actors

Non-State actors, whether groups or individuals, can have a significant impact through cyber-activity, thanks to globalization and interconnectivity.[72] There are a vast range of non-state actor goals in the use of cyber-means: recruitment, financing, training, motivation, propaganda

---

[68] Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[69] ICRC, *International Humanitarian Law and the Challenges* ... 42; Evans et al., *Cybersecurity: Mapping the Ethical* ... 4.

[70] ICRC, *International Humanitarian Law and the Challenges* ... 42.

[71] Cath, Glorioso, and Taddeo, *NATO CCD COE Workshop* ...11; Lubell, "Lawful Targets in Cyber Operations" … 272; Goldsmith, "How Cyber Changes the Laws of War." ... 134; Evans et al., *Cybersecurity: Mapping the Ethical Terrain*… 18; Dipert, 'The Ethics of Cyberwarfare' ... 390.

[72] Blank, "International Law and Cyber Threats from Non-State Actors." ... 407.

distribution, information collection, planning and organizing, command and control, and even cyber-attacks.[73] When the non-state actor has malicious intent, such as criminal groups or terrorists, cyber-capabilities can be leveraged to produce large-scale effects by a relatively small group that can risk international peace and security.[74] While malicious non-state actors have thus far found cyberspace best used as a concealed hideout and as a dispersed command and control system,[75] there are allegations that ISIS is trying to acquire an offensive cyber-warfare capability.[76]

As we began to explore earlier in this paper, there are particular attribution and distinction issues that arise when non-state actors are involved in conflict. These complications exist already in traditional physical conflict, as IHL is largely constructed with the Westphalian premise that the state is the prime actor, and are further complicated when transferred into cyberspace. A victim state already has a difficult time discerning where the cyber-attack came from, now it must also attribute the attack between the host state or a malicious non-state actor to ensure it's response it justified.[77] But before the victim state can respond, it must then determine the combatant status of the malicious non-state actor to see if it can be considered a legal military objective or must be protected as a civilian entity. Malicious non-State actors, including

---

[73] DeLuca, "The Need for International Laws of War… 291. http://digitalcommons.pace.edu/pilronline/34/; UN, 2013 *Report of the GGE* ... 7.

[74] UN, 2015 Report of GGE … 6; Lin, 'Cyber Conflict and International Humanitarian Law'… 521.

[75] Evans et al., *Cybersecurity: Mapping the Ethical Terrain* … 31.

[76] Eric Dion, 'E- Info Ops: Fighting Terrorism with Cyber Ideas', *Conference of Defence Associations Institute*, November 25, 2015, https://www.cdainstitute.ca/en/blog/entry/e-info-ops-fighting-terrorism-with-cyber-ideas.

[77] Goldsmith, "How Cyber Changes the Laws of War." ... 135; Blank, "International Law and Cyber Threats from Non-State Actors." ... 417.

'hacktivists,' that launch cyber-attacks and are not affiliated with a state in the armed conflict do not currently benefit from combatant status under IHL.[78]

Under *lex lata*, non-state actors are normally not subject to *jus ad bellum* and *jus in bello* principles. This of course makes some logical sense as malicious non-state actors do not conform to IHL during conflict and thus should not benefit from the 'belligerent immunity' imparted on armed forces.[79] Only when a malicious non-state actor can be linked to a state in the conflict, does IHL potentially apply. In these instances, the applicability of IHL would depend not the nature and duration of the attack. A single attack would likely be considered a criminal act and a sustained series of attacks could justify a use of force in response.[80] In a conflict between a state and a non-state actor, current international law creates an asymmetry where the state must abide by the IHL and the non-state actor does not, hence encouraging lawlessness on the part of the non-state actor to overcome any resource or organizational disadvantage it might have. Again, only domestic criminal laws may be able to deal with the actions of the malicious non-state actor.[81]

Note that none of these confusing IHL issues involving malicious non-state actors are limited to the confines of cyberspace. Given the rise of importance and capability of non-state actors within the international community, for good and evil, some consider it troubling that international law continues to use a state-centric view rather than a transnational approach. Law

---

[78] Blank, "International Law and Cyber Threats from Non-State Actors." ... 425, 428-32; Padmanabhan, "Cyber Warriors and the Jus in Bello." ... 296; DeLuca, "The Need for International Laws of War… 293.

[79] Andrew Jones and Gerald L. Kovacich, *Global Information Warfare: The New Digital Battlefield* (United States: Productivity Press, 2015), 303; James Andrew Lewis, *A Note on the Laws of War in Cyberspace*, (n.p.: Center for Strategic and International Studies, 2010), http://csis.org/publication/note-laws-war-cyberspace, 3.

[80] DeLuca, "The Need for International Laws of War… 309; Lewis, *A Note on the Laws of War in Cyberspace* … 3; Blank, "International Law and Cyber Threats from Non-State Actors." ... 409, 416.

[81] Jensen, Eric Talbot. "Sovereignty and Neutrality in Cyber Conflict." Fordham International Law Journal 35, no. 3 (2012): 835, 838.

scholars, lawyers, and policymakers have struggled for the past fifteen years to adapt IHL and domestic criminal law to deal with malicious non-state actors.[82]

Crime

Currently the most prevalent, harmful, and fastest growing cyber-threat is that of cyber-exploitation and cyber-espionage. Cyber-exploitation involves no disruption of the target but refers to activities that monitor or copying data from the targeted system. Examples of cyber-exploitation include the theft of intellectual property, credit card information, health records, trade secrets, and the interception of business or military and intelligence. Cyber-espionage is a subset of exploitation where the data monitored or copied is confidential information of a government or other organization.[83] While the media often refers to them as cyber-attacks, these cyber-crimes are not considered armed attacks as per *jus ad bellum* and are more properly regulated by domestic criminal law rather than IHL. Even cyber-exploitation and cyber-espionage efforts that are conducted by states in preparation for a later conflict are not considered armed attacks and the 'offending' states understands that they are not attacking the target commensurate with *jus ad bellum.*[84]

The Tallinn Manual largely does not speak to cyber-exploitation and cyber-espionage activities outside of conflict as there is little *lex lata* apart from a small number specific international legal prohibitions, such as the Vienna Convention on Diplomatic Immunity

---

[82] Gjelten, "Extending the Law of War to Cyberspace."; Goldsmith, "How Cyber Changes the Laws of War." ..., 135; DeLuca, "The Need for International Laws of War … 279, 291; Blank, "International Law and Cyber Threats from Non-State Actors." ... 409; Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." … 187.

[83] Goldsmith, "How Cyber Changes the Laws of War." ... 132; von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 5; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 35; Lin, 'Cyber Conflict and International Humanitarian Law'… 519; Talbot. "Sovereignty and Neutrality in Cyber Conflict." … 832.

[84] Padmanabhan, "Cyber Warriors and the Jus in Bello."... 288; DeLuca, "The Need for International Laws of War… 281; Lewis, *A Note on the Laws of War in Cyberspace*… 1.

pertaining to attacks against a foreign embassy.[85] Rule 66 (Cyber Espionage) of the Tallinn Manual deals only with cyber-espionage during an armed conflict.[86] Espionage or theft of intellectual property has never been considered *casus belli* (customary or legitimate reason for going to war) or as an armed attack.[87] The state response to espionage has traditionally been the reduction of commerce, expulsion of diplomats or the increase of espionage efforts against the offending state.[88] There is no reason to believe that the cyber manifestations of exploitation and espionage will garner any international interest to consider these actions as *casus belli* but the absence of any firm international regulation over cyber-spying and theft has its practical drawbacks. Pragmatically, the methods of cyber-exploitation and cyber-attack are difficult to distinguish apart and a state may very well not realize the difference until the cyber-attack is perpetrated.[89]

When speaking of activities in cyberspace, the term 'cyber-attack' is frequently wielded when speaking about cyber-crime. This misuse of the term 'cyber-attack' is proving to be dangerous as these so-called cyber-attacks are now being studied through an IHL lens when it is unnecessary to do so. Law enforcement is most often the most appropriate institution to deal with to cyber-crimes. Unfortunately, due to the securitization of cyberspace, there is an inclination to view all malicious cyber-activities through the prism of cyber-warfare. We risk the chance that

---

[85] Schmitt, Tallinn Manual… 36; Jones and Kovacich, *Global Information Warfare* ... 304; Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations*… 285; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 35; 'What Limits Does the Law of War Impose on Cyber Attacks?', ICRC; Ingo Ruhmann, 'Cyber War: Will It Define the Limits to IT Security?', *International Review of Information Ethics* 20 (December 2013): 13.

[86] Schmitt, *Tallinn Manual*... 192-4.

[87] Blank, "International Law and Cyber Threats from Non-State Actors." ... 415; Dipert, "Distinctive Ethical Issues of Cyberwarfare," … 34; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 35.

[88] Dipert, 'The Ethics of Cyberwarfare'… 389; Dipert, 'Other-than-Internet (OTI) Cyberwarfare'... 48.

[89] Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." … 190-1; Goldsmith, "How Cyber Changes the Laws of War." ... 135.

states may overreact to cyber-exploitation and respond disproportionately.[90] As von Heinegg warns, "…when one only has a hammer, most problems look like nails."[91]

Most malicious cyber-activity today is best described as cyber-crime and does not meet the threshold of an armed attack.[92] While law enforcement is the appropriate tool to fight crime, they must first be enabled in order to combat cyber-crime. Given the nature of cyberspace, the conflicting patchwork of existing domestic laws, and the global trend towards multilateral agreements; the establishment of international cyber-crime laws may be the best way to enable law enforcement in their fight against cyber-crime.[93] Baring the establishment of international cyber-crime law, it may be possible that the IHL can be supplemented with use of force options of a lower intensity in order to deal with less dangerous cyber-activities.[94] Of course this paper shows that creating such an appendage to the IHL would take significant work and time; likely more effort than creating a cyber-crime regime from scratch.

CONCLUSION

Early theorists dreamt that cyberspace would be an environment free of borders and state control.[95] The pernicious use of cyberspace has quickly shown the global community that some form of control is necessary.

This paper examined five of the most urgent and important legal obstacles to the regulation of cyber-conflict. It was shown that attribution was not a legal problem and that

---

[90] Lubell, "Lawful Targets in Cyber Operations" … 259; Evans et al., *Cybersecurity: Mapping the Ethical Terrain* …-20.

[91] von Heinegg, 'The Tallinn Manual and International Cyber Security Law'… 4.

[92] Evans et al., *Cybersecurity: Mapping the Ethical Terrain* …19.

[93] DeLuca, "The Need for International Laws of War… 305.

[94] Banks, "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." … 197.

[95] Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations…* 19.

technical professionals have largely solved this problem. The challenges of legal definition of IHL terminology, for terms like 'object' and 'use of force,' are not limited to discussion of cyber-conflict and these legal definition challenges have plagued IHL since their inception.[96] Problems of distinction were found to be incompatible with efforts to simply interpret *lex lata* and would require sustained effort to establish *lex ferenda*. Combining the challenges of both distinction and legal definition, the regulation of malicious non-state actors was shown to be both a legacy obstacle of IHL and an issue that would likely require new laws to address.[97]

Finally, cyber-crime was shown to be a particularly consequential issue to promptly address as it accounts for the predominance of current malicious cyber-activities. As cyber-exploitation and cyber-espionage largely falls outside of *jus ad bellum* and *jus in bello* norms, there is no need for the international community to "open up" IHL to address the issue. The establishment of international norms around the regulation of cyber-crime therefore could be accomplished much faster, it would deescalate the militarization of cyberspace, and it also would provide some additional legal control over cyber-conflict. Such an approach would also have beneficial second order effects to other cyber-security problems (i.e. non-state actors).

---

[96] Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

[97] Captain (Navy) Geneviève Bernatchez (legal officer), telephone conversation with the author, 22 April 2016.

BIBLIOGRAPHY

Ackerman, Robert K. "Air Force Cyber Faces Familiar Challenges." *Signal* March 2016,: 16–17.

Banks, William. "The Role of Counterterrorism Law in Shaping Ad Bellum Norms for Cyber Warfare." *International Law Studies* 89 (2013): 157–97.

Barrett, Edward T. "The Applicability of the Just War Tradition to Military Cyber Operations." Edited by Ludovica Glorioso and Anna-Maria Osula. *Workshop on Ethics of Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014. https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf.

Blank, Laurie R. "International Law and Cyber Threats from Non-State Actors." *International Law Studies* 89 (2013): 406–37.

Boer, Lianne J. M. "'Restating the Law "As It Is"': On the Tallinn Manual and the Use of Force in Cyberspace." *Amsterdam Law Forum* 5, no. 3 (2013): 4–18.

Boothby, Bill. "Law, Ethics and Cyber Warfare." Edited by Ludovica Glorioso and Anna-Maria Osula. *Workshop on Ethics of Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014. https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf.

Braman, Sandra. "Cybersecurity Ethics at the Boundaries." *YouTube* streaming. November 21, 2013. Posted March 30, 2016. http://youtu.be/c0Sfa21CsA0. Workshop of Ethics of Cyber Conflict, Rome, Italy.

Cath, Corinne J. N., Ludovica Glorioso, and Maria Rosaria Taddeo. *NATO CCD COE Workshop on "Ethics and Policies for Cyber Warfare" (Magdalen College, Oxford)*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014. https://ccdcoe.org/sites/default/files/multimedia/pdf/report_workshop_on_ethics_publication.pdf.

DeLuca, Christopher D. "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors." *Pace International Law Review Online Companion* 3, no. 9 (January 1, 2013): 278–315. http://digitalcommons.pace.edu/pilronline/34/.

Diakonia International Humanitarian Law Resource Centre. "Basic Principles of IHL." October 30, 2013. Accessed April 20, 2016. https://www.diakonia.se/en/ihl/the-law/international-humanitarian-law-1/introduction-to-ihl/principles-of-international-law/.

Dion, Eric. "E-Info Ops: Fighting Terrorism with Cyber Ideas." *Conference of Defence Associations Institute*. November 25, 2015. https://www.cdainstitute.ca/en/blog/entry/e-info-ops-fighting-terrorism-with-cyber-ideas.

Dipert, Randall R. "Distinctive Ethical Issues of Cyberwarfare." Edited by Ludovica Glorioso and Anna-Maria Osula. *Workshop on Ethics of Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2014. https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf.

—. "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy." *Journal of Military Ethics* 12, no. 1 (April 2013): 34–53. doi:10.1080/15027570.2013.785126.

—. “The Ethics of Cyberwarfare.” *Journal of Military Ethics* 9, no. 4 (December 2010): 384–410. doi:10.1080/15027570.2010.536404.

Dunlap, Charles J. “Some Re Ections on the Intersection of Law and Ethics in Cyber War.” *Air & Space Power Journal* 27, no. 1 (2013): 22–43.

Durante, Massimo. “Violence, Just Cyber War and Information.” Edited by Ludovica Glorioso and Anna-Maria Osula. *Workshop on Ethics of Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, n.d. https://ccdcoe.org/publications/ethics-workshop-proceedings.pdf.

Evans, Nicholas g., S. Brandt Ford, Adam C. Gastineau, Adam Henschke, Michael Keelty, and Levi J West. *Cybersecurity: Mapping the Ethical Terrain*. Australian National University, Acton: National Security College, 2014.

Gjelten, Tom. “Extending the Law of War to Cyberspace.” September 22, 2010. Accessed April 23, 2016. http://www.npr.org/templates/story/story.php?storyId=130023318.

Glennon, Michael J. “The Road Ahead: Gaps, Leaks and Drips.” *International Law Studies* 89 (2013): 362–86.

Goldsmith, Jack. “How Cyber Changes the Laws of War.” *European Journal of International Law* 24, no. 1 (February 1, 2013): 129–38. doi:10.1093/ejil/cht004.

International Committee of the Red Cross. “Commentary of 1987 General Protection of Civilian Objects.” 1987. Accessed May 6, 2016. https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=5F27276CE1BBB79DC12563CD00434969.

—. “Cyber Warfare.” January 14, 2016. Accessed March 30, 2016. https://www.icrc.org/en/war-and-law/conduct-hostilities/cyber-warfare.

—. “What Limits Does the Law of War Impose on Cyber Attacks?” July 1, 2013. Accessed March 30, 2016. https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

—. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*. Geneva: International Committee of the Red Cross, 2015. https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

International Court of Justice. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*. 226th ed. n.p., 1996.

Jensen, Eric. “Cyber Sovereignty: The Way Ahead.” *Talbot Texas International Law Journal* 50, no. 2/3 (2015): 275.

—. “Sovereignty and Neutrality in Cyber Conflict.” *Fordham International Law Journal* 35, no. 3 (2012): 815–41.

Jones, Andrew and Gerald L. Kovacich. *Global Information Warfare: The New Digital Battlefield*. United States: Productivity Press, 2015.

Jontz, Sandra. “Cyber Ethics Vex Online Warfighters.” *Signal* January 2016,: 32–33.

Kanuck, Sean. “Sovereign Discourse on Cyber Conflict Under International Law.” *Texas Law Review* 88, no. 7 (June 2010): 1571–97.

Kessler, Oliver and Wouter Werner. “Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare.” *Leiden Journal of International Law* 26, no. 04 (November 8, 2013): 793–810. doi:10.1017/s0922156513000411.

Kimball, Spencer. “NATO Moves to Apply Armed Conflict Law to Cyber Warfare.” *Deutsche Welle* (Deutsche Welle), July 2, 2014. http://www.dw.com/en/nato-moves-to-apply-armed-conflict-law-to-cyber-warfare/a-17754359.

Klein, Adam. “Tallinn 2.0 and a Chinese View on the Tallinn Process.” *Lawfare*. January 14, 2016. https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process.

Lewis, James Andrew. *A Note on the Laws of War in Cyberspace*. n.p.: Center for Strategic and International Studies, 2010. http://csis.org/publication/note-laws-war-cyberspace.

Lin, Herbert. “Cyber Conflict and International Humanitarian Law.” *International Review of the Red Cross* 94, no. 886 (June 2012): 515–31. doi:10.1017/s1816383112000811.

Lubell, Noam. “Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?” *International Law Studies* 89 (2013): 252–75.

Margulies, Peter. “Sovereignty and Cyber Attacks: Technology’s Challenge to the Law of State Responsibility.” *Melbourne Journal of International Law* 14 (2013): 496–519.

Moens, Alexander. *Cybersecurity Challenges for Canada and the United States*. Vancouver, BC: Fraser Institute, 2015.

NATO Cooperative Cyber Defence Centre of Excellence. “Prof. Luciano Floridi - the Ethics of Cyber-Conflicts in Hyperhistorical Societies.” *YouTube*. January 8, 2014. Posted March 2, 2016. http://www.youtube.com/watch?v=c9417JcQeF4.

—. “Prof. Sandra Braman - Cybersecurity Ethics at the Boundaries.” *YouTube*. January 8, 2014. Posted March 2, 2016. http://www.youtube.com/watch?v=c0Sfa21CsA0.

Padmanabhan, Vijay M. “Cyber Warriors and the Jus in Bello.” *International Law Studies* 89 (2013): 288–308.

Pagallo, Ugo. “Three Legal Challenges of Informational Warfare.” *YouTube* streaming. November 21, 2013. Posted March 30, 2016. http://youtu.be/aJmd28nVfdU. Workshop on Ethics of Cyber Conflict, Rome, Italy.

Raboin, Bradley. “Corresponding Evolution: International Law and the Emergence of Cyber Warfare.” *Journal of the National Association of Administrative Law Judiciary* 31, no. 2 (October 15, 2011): 602–68. http://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5.

Rowe, Neil C. “Ethics of Cyberwar Attacks.” In *Cyber warfare and cyber terrorism*, by Lech Janczewski and Andrew Colarik, 105–11. n.p.: Information Science Reference, 2007.

Ruhmann, Ingo. “Cyber War: Will It Define the Limits to IT Security?” *International Review of Information Ethics* 20 (December 2013): 4–15.

Schmitt, Michael N. “Tallinn Manual.” *YouTube* streaming. September 29, 2012. Posted March 30, 2016. http://youtu.be/wY3uEo-Itso. CyCon 2012, Tallinn, Estonia.

—. “International Law and Cyberwar: A Response to the Ethics of Cyberweapons.” *Ethics & International Affairs*. February 10, 2014. http://www.ethicsandinternationalaffairs.org/2014/international-law-and-cyberwar-a-response-to-the-ethics-of-cyberweapons/.

—. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

—. “Classification of Cyber Conflict.” *International Law Studies* 89 (2013): 233–51.

—. “International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed.” *Harvard International Law Journal* 54 (December 2012): 13–37.

—. “Rewired Warfare: Rethinking the Law of Cyber Attack.” *International Review of the Red Cross* 96, no. 893 (March 2014): 189–206. doi:10.1017/s1816383114000381.

Shackelford, Scott J. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge: Cambridge University Press, 2014.

Snyder, Melanie G. “Cyber-Ethics: Pirates in the Classroom.” *Science Activities* 41, no. 3 (2004): 3–4.

United Nations. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/172.

—. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 2013. http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156.

United States of America. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Washington, DC: United States of America, 2011. https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf.

von Heinegg, Wolff Heintschel. “The Tallinn Manual and International Cyber Security Law.” In *Yearbook of International Humanitarian Law Volume 15,* edited by T. D. Gill, R. Geiß, R. Heinsch, T. McCormack, C. Paulussen, and J. Dorsey, 3–18. The Hague, The Netherlands: T.M.C. Asser Press, 2013.

Weisman, Vivien Lesnik and Meredith Raithel Perry. *The Hacker Wars*. Directed by Vivien Lesnik Weisman. n.p.: Vitagraph Films, 2014. Streaming, 91 mins.

Convention relative to the Treatment of Prisoners of War., August 12, 1949.

Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, October 18, 1907.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, June 8, 1977.