Journal of Military and Strategic Studies

VOLUME 20, ISSUE 1

Annual Award of Excellence 2019
First Place

The Devil is in the Details: An Examination of Hybrid Cyber Operations and International Law

Dean Coslovi

Introduction

According to philosopher Thomas Hobbes, the state of nature is *bellum omnium contra omnes*, or "the war of all against all."[1] Hobbes believed that the only way to avoid this undesirable state of nature was to enter into mutual agreements in order to exit the state of nature and enter into civil relations amongst human beings. International law has adopted this viewpoint on an international level by creating laws to govern the interactions between states, including the laws of armed conflict (LOAC).[2] One of the fundamental tenets of international law, which is designed to avoid a "war of all against all," is Article 2(4) of the United Nations Charter which states that "[a]ll Members shall

[1] Thomas Hobbes, *De Cive* (Copenhagen: Titan Read, 2015), chapter 1, para 12.
[2] For the purposes of this paper the "laws of armed conflict (LOAC)" will refer to both international treaties governing the conduct of military operations and customary international humanitarian law.

ISSN : 1488-559X

refrain in their international relations from the threat or use of force."[3] The only exception to this prohibition on the use of force is if a nation is acting in self-defence as mandated by Article 51 of the UN Charter, or if the use of force is sanctioned by the UN Security Council.[4]

In order for a nation to legally use force in self-defence, two criteria must be met. First, the nation must show that it has been the victim of an "armed attack."[5] This entails that a certain threshold of damage and destruction must be experienced by the targeted nation. In order to differentiate a "use of force" from an "armed attack," the "scale and effects" or damage and destruction caused by the incident must be examined.[6] This is critical because a "use of force" is not sufficient to warrant a retaliatory use of force in the context of self-defence. Secondly, if the scale and effects of the attack are deemed sufficient to be considered an "armed attack," the nation wishing to use force in self-defence must then prove who is responsible for the attack. This second condition, known as attribution, must be met in order for a nation to legally use force in self-defence.

The purpose of this discussion is to clearly identify how hybrid cyber operations pose distinct issues for international law regulating the resort to the use of force in the context of self-defence. To accomplish this task, this article will highlight how hybrid cyber operations are able to circumvent the necessary *jus ad bellum* legal justifications for self-defence set forth in international law. Specifically, the inherent issues surrounding the classification of cyber "uses of force" and cyber attribution seemingly

[3] Charter of the United Nations, "Chapter I: Purposes and Principles," accessed 6 April 2019, http://legal.un.org/repertory/art2.shtml, art. 2, para 4.
[4] Charter of the United Nations, "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," accessed 9 April 2019, http://www.un.org/en/sections/un-charter/chapter-vii/index.html, art. 51.
[5] Charter of the United Nations, "Chapter VII: Action With Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," art. 51.
[6] "Scale and effects" is a legal term that originates from the International Court of Justice (ICJ) judgement regarding Nicaragua v. United States of America. In this case, the ICJ noted that there is a "substantive difference between a use of force and an armed attack and that not all uses of force warrant unilateral self-defense." *See* International Court of Justice, "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)," Judgement, 27 June 1986, para. 195. & Priyanka R. Dev, "'Use of Force' and 'Armed Attack' thresholds in Cyber Conflict: The Looming Definitional Gaps, and the Growing need for Formal U.N. Response," *Texas International Law Journal* 50, 2 (2015): p. 393.

negate the possibility for the victims of hybrid cyber operations to construct a *casus belli* that abides by international law.[7] As a result, nations can seemingly perpetrate hybrid cyber operations with little fear of being held internationally accountable for such actions. In this way, the use of hybrid cyber operations undermines the deterrent value of conventional military power.

These issues will be addressed in the first section while the second section will be devoted to examining empirical case studies that highlight the theoretical issues that have been raised. Once these cases have been analyzed, it will become evident how international law impedes the ability of the victims of hybrid cyber operations to legally use force in response to these acts of aggression.

1 International Law, Hybrid Cyber Operations and the *Tallinn Manual*

International experts are attempting to reconcile the domain of cyberspace with international law and the ways in which hybrid cyber operations pose new challenges for the conventional LOAC. Currently, there are no universally accepted treaties specifying how international law should be applied to cyberspace.[8] However, a robust attempt has been made to reconcile international law with cyberspace by the authors of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare.*

This manual shows how existing international law could be applied to cyberspace. The *Tallinn Manual*'s legal positivist framework means that the legal reasoning utilized within the manual strictly follows the conventions and rules of existing international law. However, as this paper will demonstrate, the nuances and non-physical nature of cyberspace are ill-suited to a mechanical and inflexible application of contemporary international law. As such, examining the *Tallinn Manual*'s use of this legal positivist approach to international law is necessary both to understand how international law could be applied to cyberspace, and why such an application would be ineffective.

[7] The term *casus belli* can be translated as "a case for war" and refers to the notion of providing justification for entering into an armed conflict or using force.

[8] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat (Online)*, 31 July 2017, accessed 2 August 2018, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

1.1 The *Tallinn Manual* and International Law

The development of the contemporary LOAC has resulted from a shared belief amongst nations that interactions between states and actions undertaken in armed conflicts are subject to specific norms of acceptable behaviour. These rules and regulations have evolved over time in tandem with the development and implementation of new means and methods of warfare. While the ratification of new international law can occur at a glacial pace, the legal reasoning utilized in the LOAC is designed to incorporate new developments in weapon technology and warfare within the existing LOAC framework.

For example, in 1996 the International Court of Justice's (ICJ) report on the *Legality of the Threat or Use of Nuclear Weapons* affirmed that "the established principles and rules of international humanitarian law… apply to all forms of warfare, and to all kinds of weapons, those of the past, those of the present and those of the future."[9] In this way, even though the LOAC cannot predict how new weapon systems will develop, the legal framework of the LOAC maintains that new weapon systems will be subject to the basic rules and regulations of existing international laws.

This is precisely the same legal positivist reasoning utilized by the International Committee of Experts who authored the *Tallinn Manual* in their attempt to reconcile contemporary international law with the realm of cyberspace. Legal positivism is the dominant legal approach to both domestic and international law. It emphasises a strict adherence to the rules and regulations specified by the individual clauses that compose the overall corpus of the law.[10] In this way, valid legal reasoning, which demarcates acceptable and unacceptable legal actions, is dictated by the rules and regulations of the law itself.[11] As such, adhering to a legal positivist framework results in the rigid understanding and application of law. It also makes use of previous cases of legal precedence in its legal reasoning. While this rigid application of existing international

[9] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, 8 July 1996, ICJ Reports 1996, para 86.
[10] Leslie Green, "Legal Positivism," in *The Stanford Encyclopedia of Philosophy,* Spring 2018 Edition, ed., Edward N. Zalta, accessed 6 March 2019, https://plato.stanford.edu/entries/legal-positivism/#4.
[11] Green, "Legal Positivism."

law would seem ill-suited to dealing with the nuances of hybrid cyber operations, this legal positivist approach to cyber law does have significant benefits.

By adopting a legal positivist approach to international law and cyber space, the *Tallinn Manual* is able to clearly demonstrate the *lex lata,* or the law currently applicable to cyberwarfare.[12] The greatest strength of the *Tallinn Manual* is the legal reasoning it applies to the four core principles of the LOAC; namely, proportionality, distinction, the prohibition on unnecessary suffering, and military necessity. These four principles are considered to be customary international law, and thus they impose normative standards of behavior upon all actors engaged in hostilities.

To clarify this point, the *Tallinn Manual* also cites the ICJ's legal reasoning on the *Legality of the Threat or Use of Nuclear Weapons* to conclude that "the general rules that determine the legality of weapons will also determine the lawfulness of cyber methods and means of warfare."[13] By applying the legal reasoning of existing international law to the realm of cyberspace, the *Tallinn Manual* has made it clear that the core principles of the LOAC are universally binding and that they impose normative standards of behaviour upon all forms of warfare. Thus, despite an absence of any international treaty relating to cyberwarfare, the legal positivist approach utilized by the *Tallinn Manual* asserts that cyber means and methods of warfare must abide by the four "intransgressible" principles that form the basis of the LOAC.[14]

To illustrate this point, consider Rule 108 of the *Tallinn Manual* regarding belligerent reprisals. The *Tallinn Manual* states that belligerent reprisals, whether cyber or kinetic, can "occur only during an armed conflict… in response to a violation of the law of armed conflict," in an attempt "to induce or compel compliance with the law by the enemy."[15] However, this does not entail that a case of belligerent reprisal allows a state to carry out the reprisal unreservedly. This is because, as the *Tallinn Manual* highlights, belligerents in any armed conflict are constrained by the incontrovertible

[12] Michael N. Schmitt, *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations*, (New York: Cambridge University Press, 2017), p. 2.
[13] Schmitt, *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations*, section 5, para 1.
[14] Schmitt, rule 93, para 2.
[15] Ibid, rule 108, para 3 and 2.

core principles of "customary international law that binds all states."[16] As such, even if a cyber reprisal was carried out in the course of an armed conflict, the core principles of the LOAC would necessarily constrain how a state could legally undertake the cyber reprisal. As this example highlights, the greatest strength of the *Tallinn Manual* is the legal positivist reasoning that it utilizes to show why cyber means and methods of warfare are subject to, and thus constrained by, the core principles of the LOAC.

In this way, the *Tallinn Manual* approach shows how the core principles of the LOAC and other key features of existing international law are applicable to the domain of cyberspace. So far, other attempts to ratify new international laws regulating cyberspace have been vetoed by certain members of the international community.[17] Nevertheless, the strength of this approach is such that some legal scholars and professionals have begun to view this approach as the best way to understand how international law should be applied to cyberspace.[18] However, even if one deems that the *Tallinn Manual* is able to adequately reconcile the application of international law to cyberspace, international law itself is fundamentally unequipped to deal with the unconventional strategy of hybrid warfare.

1.2 Hybrid Cyber Operations and Self-Defence

Hybrid warfare has recently proven to be an extremely effective method of implementing an aggressive foreign policy whilst avoiding the traditional restrictions imposed by international law. The efficacy of hybrid warfare stems from the practice of employing unconventional and asymmetric means of warfare that blur the distinction between the states of peace and war. These unconventional and asymmetric means make it difficult for the victims of hybrid warfare, as well as the wider international

[16] Ibid, rule 108, para 4.
[17] United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," (24 June 2013), UN Doc A/68/98.; & United Nations General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," (22 July 2015), UN Doc A/70/174.
[18] Stephen Hill, "Briefing on NATO and International Law," (presentation, Simon Fraser University NATO Field School, Brussels, 26 June 2018). & Chelsey Slack, "Briefing on NATO and Cybersecurity," (presentation, Simon Fraser University NATO Field School, Brussels, 28 June 2018).

community, to determine how to respond to these acts of aggression within the strict parameters of international law.

While hybrid warfare can be conducted using a myriad of means and methods, the non-physical domain of cyberspace has recently emerged as the ideal medium in which to carry out hybrid military operations. [19] Hybrid cyber operations can come in many different forms, ranging from information-based warfare to cyberattacks on critical national infrastructure. One of the main benefits of these types of cyber operations is that the vast majority can be carried out remotely, mitigating the risks associated with deploying men and material for operations involving kinetic force. [20] Moreover, cyber operations have the capability to disrupt and/or destroy key enemy targets in ways that would be nearly impossible using conventional means.

While the benefits of utilizing hybrid cyber operations are substantial, perhaps the most significant advantage conferred by cyber operations is the manner in which these operations circumvent the existing international law regulating the use of force in self-defence. Hybrid cyber operations are able to exploit this area of international law because in order for a nation to legally use force in self-defence it is necessary for: a) an "armed attack" to have occurred, and b) the perpetrators of this "armed attack" to be positively identified.

While these conditions are reasonable for regulating conventional military operations, they become nearly impossible to fulfill in the context of hybrid cyber operations. This is because the scale and effects of hybrid cyber operations rarely even qualify as a "use of force", let alone an "armed attack." However, even if a cyber operation were to qualify as a "use of force", "[n]owhere is the term 'use of force' clearly defined" in international law.[21]

---

[19] Diego A. Ruiz Palmer, "Back to the Future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons," *NATO Defense College Research Division,* No. 120 (October 2015): p. 2; Sona Rusnakova, "Russian New Art of Hybrid Warfare in Ukraine," *Slovak Journal of Political Sciences* 17, no. 3-4 (2017): p. 348.

[20] Palmer, "Back to the Future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons," p. 2.

[21] Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War (2nd Edition).* (New York: Cambridge University Press, 2016), p. 682.

Although the term "use of force" is specified in Article 2(4) of the U N Charter, the Article does not explicitly demarcate the threshold at which a "use of force" has been perpetrated.[22] Furthermore, the term "armed attack" has no "legal definition nor universally accepted definition."[23] Neither the UN Charter nor the contemporary LOAC legally define the circumstances necessary to bring about the existence of an "armed attack." Therefore, even if one accepts the *Tallinn Manual*'s assertion that a "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force," it is difficult to precisely determine when the "scale and effects" of a cyberattack would rise to the level of an "armed attack."[24]

Even if one were to reference the scale and effects associated with a previous classification of an "armed attack" from a case of precedence in international law, the nature of hybrid cyber operations entails that one would then be faced with the attribution problem. Put simply, the attribution problem is the issue of determining who is responsible for perpetrating a hybrid cyber operation. Without attribution, there is no clear target for a nation to defend themselves against. In this way, even if a cyber operation rises to the level of an "armed attack", the rules of international law are such that the burden of proving who is responsible for the attack rests with the party that brings the accusation forward.[25] However, the non-physical nature of cyberspace, the complexities of computing technology, and the deliberate attempts by perpetrators to hide their involvement render conclusive attribution in cyberspace to be, at best, a guessing game.[26] For these reasons, attributing cyber responsibility can only deal in "degrees of certainty, not absolutes."[27]

---

[22] Charter of the United Nations, "Chapter I: Purposes and Principles," art. 2, para 4.
[23] Katharina Ziolkowski, "NATO and cyber defence," *International Law and Cyberspace,* edited by Russell Buchan and Nicolas Tsagourias. (North Hampton: Edward Elgar Publishing Inc., 2015), p. 434.
[24] Schmitt, rule 69.
[25] Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," *Texas International Law Journal* 50, 2 (2015): p. 272.
[26] Jan Dyment, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence," *Security Intelligence,* 28 December 2018, https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/; & Lily Hay, "Hacker Lexicon: What is the Attribution Problem?" *Wired,* 24 December 2016, https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/; & Symantec Expert Perspectives, "The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks," *Symantec Corp,* 3

For example, one of the most common techniques for concealing the origins of cyber operations is the technique of spoofing.[28] With this technique, a perpetrator is able to make it appear as if the origin of a cyber operation is from a source unrelated to the true origin of the cyber action.[29] This spoofing of the true origin of the cyber operation can be done millions of times as the cyber operation is directed through networks and computer systems around the globe.[30] This level of technical complexity and the short life span of digital evidence, which is often located in foreign countries, makes it extremely difficult to determine the physical location that the cyber operation originated from.[31]

However, even if one is able to conclusively determine that a cyber operation originated from within a state, this still does not prove that the state is responsible for the cyber operation. The imprecise nature of technical cyber attribution entails that a state will inevitably have a certain level of plausible deniability.[32] For instance, a state can simply claim that the origin of the cyber operation was misattributed and that the state itself was the victim of cyber spoofing.[33]

Furthermore, determining that a cyber operation originated from within a state does not prove that the individual(s) who carried out the operation were doing so on behalf of the state itself.[34] As the ICJ determined in the *Corfu Channel* case, "it cannot be concluded from the mere fact of the control exercised by a State over its territory… that the State necessarily knew, or ought to have known any unlawful act perpetrated

---

October 2018, https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks.

[27] Hay, "Hacker Lexicon: What is the Attribution Problem?"

[28] Dyment, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence."

[29] Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," p. 264.

[30] Jair Aguirre, Benjamin Bourdreaux, Michael S. Chase, John S. Davis II, Geoffrey McGovern, Cordaye Ogletree, Johnathan William Welburn, *Stateless Attribution: Toward International Accountability in Cyberspace* (Santa Monica: RAND Corporation, 2017), p. 10.

[31] Nicolas Tsagourias, "Cyber attacks, self-defence and the problem of attribution," *Journal of Conflict & Security Law* 17, 2 (2012): p. 234.

[32] Dyment, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence."

[33] Ibid.

[34] Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," p. 264.

therein."[35] For these reasons, the act of determining where a cyber operation physically originated from, is not sufficient for attributing the operation to a state.

Another complicating factor arises from the fact that cyber operations can be carried out by individuals or groups. This allows states the ability to claim that the individual or group responsible for the cyber operation was acting without the authority of the state and was a non-state actor. As noted by Rule 17 of the *Tallinn Manual*, "cyber operations by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own."[36]

Proving that a non-state actor carried out a cyber operation under the "direction or control" of the state is extremely difficult in practice. This is made clear in the ICJ's statement regarding attribution in the *Nicaragua Case* that, "the problem is not… the legal process of imputing the act to a particular State…but the prior process of tracing the material proof of the identity of the perpetrator."[37] Furthermore, the ICJ's judgment in the *Nicaragua Case* also makes it clear that in order for an individual or group be consider to be under state control, the relationship between the individual(s) or group and the state must be one of complete dependence and control.[38] Again, this criteria is nearly impossible to satisfy in the context of cyber operations because evidence of this dependence and control relationship is extremely difficult to establish. This becomes more challenging when one considers that any evidence gathering missions would almost inevitably require the cooperation of the accused state and a willingness to provide access to sensitive state information. As a result, seemingly the only conclusive way to prove cyber attribution is if a state formally accepts responsibility for the operation. However, this is *extremely* unlikely to happen in practice.

To summarize, victims of hybrid cyber operations and the international community are faced with a two-pronged dilemma in legally establishing the right to use force in self-defence. This dilemma stems from the requirement that it must be

[35] International Court of Justice, *The Corfu Channel Case (Merits),* Judgments, Merits, 9 April 1949, p. 18.
[36] Schmitt, rule 17.
[37] International Court of Justice, "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)," para 57.
[38] Ibid, para 109 and 111.

shown that: a) an "armed attack" has occurred and b) the attack can be positively attributed. However, as shown above, meeting both of these criteria is a near impossibility due to the nature of hybrid cyber operations. Even if the scale and effects of a cyber operation reach the threshold of an "armed attack," it is virtually impossible to conclusively prove who is responsible for the attack. Thus, nations are seemingly unable to legally use force in response to hybrid cyber operations without committing an internationally wrongful act. Consequently, hybrid cyber attackers are able to exploit the existing requirements of international law, making cyber operations an increasingly appealing means of warfare.

2 Case Studies

Having established the theoretical issues concerning hybrid cyber operations and international law in Section I, Section II will be devoted to grounding these theoretical issues with empirical case studies. Specifically, in order to make it clear why existing international law is ill-suited to the complexities of hybrid cyber operations, this paper will closely examine two case studies: the DDoS cyberattacks launched against Georgia in 2008, and the Stuxnet worm that destroyed Iranian nuclear centrifuges in 2009-10. These are two of the limited number of non-theoretical cases highlighted in the *Tallinn Manual.* As such, these two cases are exemplars for how international legal scholars have begun to conceptualize warfare in cyberspace.

Through an examination of these two cases it will become clear why the *Tallinn Manual's* legal positivist interpretation of international law is fraught with inherent issues of applicability when faced with the complexities of real-world cyber operations. Once these issues have been made clear, the potential developments of increasingly sophisticated cyber operations will be briefly examined. This will make it clear how hybrid cyber operations are likely to become progressively more problematic in the future and the challenges this poses for international law in the future.

2.1 Georgian Cyberattacks

In the early summer of 2008, the nation of Georgia suffered a series of massive cyberattacks that targeted the networks of the Georgian government as well as its

banks, media outlets, transportation services and communication companies.[39] In total, it is estimated that roughly thirty-five percent of all of Georgia's internet networks were affected by these attacks.[40] The specific type of cyberattacks that were used are known as a Distributed Denial of Service Attack (DDoS), and they were designed to prevent "Georgian authorities from keeping information flowing to national and international media."[41] The DDoS attacks were able to accomplish this by overloading web servers with superfluous requests.[42] By inundating the servers with numerous redundant requests, DDoS attacks prevents legitimate requests from being processed. In the case of Georgia, the widespread DDoS attacks made it nearly impossible for the Georgian government or Georgian citizens to access critical online services.

The confusion and panic caused by these cyberattacks was exacerbated by ongoing hostilities between Georgia and Russia in the South Ossetia region. Although the South Ossetia region is officially part of Georgian territory, the region has its own government that is supported by the Russian state.[43] At the time of the cyber attacks against Georgia, the conflict between Georgian troops and separatists in South Ossetia was reaching a boiling point, with physical altercations occurring throughout the summer of 2008.[44] Many Georgian government officials, including President Mikheil Saakashvili, believed that these cyberattacks were part of a Russian operation to intervene in the South Ossetia region.[45]

Fearing an imminent Russian intervention, President Saakashvili deployed Georgian troops to South Ossetia and ordered the South Ossetian capital of Tskhinvali

[39] John Markoff, "Before the Gunfire, Cyberattacks," *The New York Times,* 12 August 2008, accessed 28 March 2019, https://www.nytimes.com/2008/08/13/technology/13cyber.html.
[40] Sarah P. White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," *Modern War Institute,* 20 March 2018, accessed 27 March 2019, https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/, p. 1.
[41] Carlo Focarelli, "Self-defence in cyberspace," *International Law and Cyberspace,* edited by Russell Buchan and Nicolas Tsagourias, (North Hampton: Edward Elgar Publishing Inc., 2015), p. 259.
[42] Jim Breithaupt and Mark S. Merkow, *Information Security: Principles and Practices 2nd Edition,* (Indianapolis: Pearson Education, 2014), Chapter 2.
[43] CNN, "2008 Georgia Russia Conflict Fast Facts," *CNN,* 3 April 2018, accessed 27 March 2019, https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html.
[44] British Broadcasting Corporation, "South Ossetia Profile," *BBC News (Online),* 21 April 2016, accessed 27 March 2019, https://www.bbc.com/news/world-europe-18269210.
[45] CNN, "2008 Georgia Russia Conflict Fast Facts."

to be shelled on 7 August 2008.[46] These aggressive Georgian actions prompted a Russian military response, and an armed conflict between Russia and Georgia broke out in the South Ossetia region.[47] Shortly after the beginning of the armed conflict, Russian forces were able to overwhelm their Georgian adversaries and push them out of South Ossetia.[48] Ultimately, Russia was able to establish military bases in the South Ossetia region, and it currently maintains de facto control over the area despite the region still officially being part of Georgia.[49]

2.11 Analysis of Georgian Cyberattacks

Following the end of the 2008 Russo-Georgian War, the European Union launched an investigation into the cause of the conflict. It concluded that, "the shelling of Tskhinvali, without warning, by Georgia marked a new level of escalation and constituted a disproportionate use of armed force."[50] For this reason, the EU report concluded that in regards to the "question of whether the use of force by Georgia in South Ossetia… was justifiable under international law. It was not."[51] As such, despite the fact that there had been clashes between Georgian and Russian forces in South Ossetia prior to 7 August 2008, the EU fact-finding mission had determined that Georgia's aggressive actions violated international law and constituted an unjustifiable use of force.[52]

[46] Ibid.
[47] Ibid.
[48] British Broadcasting Corporation, "South Ossetia Profile,"
[49] Sergei Goryashko, "South Ossetia: Russia Pushes Roots Deeper into Georgian Land," *BBC,* 8 August 2018, accessed 27 March 2018, https://www.bbc.com/news/world-europe-45100160.
[50] Council of the European Union, *Independent International Fact-Finding Mission on the Conflict in Georgia: Volume I,* (Brussels: European Union, 2009), p. 612.
[51] Council of the European Union, *Independent International Fact-Finding Mission on the Conflict in Georgia: Volume I,* p. 23.
[52] British Broadcasting Corporation, "Georgia 'started unjustified war," *BBC News (Online),* 30 September 2009, accessed 18 February 2019, http://news.bbc.co.uk/2/hi/europe/8281990.stm.

The EU's conclusion is extremely important when one considers that the massive cyberattacks against Georgia began occurring in July 2008.[53] This implies that the EU's inquiry did not deem the scale and effects of the Georgian cyberattacks significant enough to qualify as an "armed attack." Thus, despite the widespread disruption and panic that the DDoS cyberattacks caused, it was determined that Georgia did not have a legal right to resort to the use of force.

In regards to attributing responsibility for the DDoS attacks against Georgia, the Russian state was widely viewed as being the most likely culprit.[54] Russia seemingly had a strong political motivation for perpetrating the cyberattacks due to the ongoing hostilities between the Georgian and Russian states.[55] Russia also had a strong military motivation as the later cyberattacks against Georgia in August seemed to coincide with Russian troop movements.[56] Furthermore, some of the IP addresses used in the cyber operation, which act as identification and location markers for computers connecting to networks, were traced to Russian state-operated companies.[57]

However, despite these circumstances, the Russian state denied any responsibility for the cyber operations.[58] The Russian government maintained that "the hacking of Georgian websites was undertaken by 'patriotic activists'…spontaneously and outside any government control."[59] In particular, the Russian hacker communities "xaker.ru" and "StopGeorgia.ru" were used to coordinate the cyberattacks and distribute the necessary hacking tools to those within these communities.[60] The nature of these hacker communities was largely decentralized, with individual hackers

[53] Stephen Korns and Joshua Kastenberg, "Georgia's Cyber Left Hook," *Parameters* 38, 4, (Winter 2008/2009): p. 60.
[54] Korns and Kastenberg, "Georgia's Cyber Left Hook," p. 65; Solis, *The Law of Armed Conflict: International Humanitarian Law in War (2nd Edition),* p. 679.
[55] Ben Buchanan and Thomas Rid, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38, 1-2, p. 23.
[56] Korns and Kastenberg, p. 60; White, "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," p. 1.
[57] Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," pp. 235-6.
[58] Ibid.
[59] David Turns, "Cyber war and the law of neutrality," *International Law and Cyberspace,* edited by Russell Buchan and Nicolas Tsagourias, (North Hampton: Edward Elgar Publishing Inc., 2015), p. 392.
[60] White, p. 6.

choosing their own targets from a generalized list.[61] Consequently, although Russian state involvement was widely suspected, the decentralized nature of the hacker communities and the absence of clear Russian government control entailed that it could not be conclusively proven that the Georgian cyberattacks were attributable to the Russian state.[62]

2.2 The Stuxnet Worm

In 2010, a computer security firm troubleshooting computers in Iran stumbled upon the "world's first digital weapon."[63] This weapon was a computer virus, known as "Stuxnet", specifically created to cause physical damage to targeted systems.[64] In the case of Stuxnet, the intended targets of the virus were the centrifuges in Iran's nuclear facilities.[65] Centrifuges are used to enrich uranium, a critical component for the production of nuclear weapons as well as nuclear power generation .[66] The virus was introduced via an infected USB device and was designed to seek out control systems within the nuclear centrifuges in order to adjust the rotational speed of the centrifuge's motors.[67] By quickly adjusting the rotational speed of the motors, the virus could cause the centrifuges to fly apart.[68]

Although it is unknown when exactly Stuxnet infected Iranian systems, inspectors from the International Atomic Energy Agency (IAEA) noted that centrifuges at the Natanz uranium enrichment plant "were failing at an unprecedented rate" in

[61] Ibid.
[62] Jon Swaine, "Georgia: Russia 'conducting cyber war,'" *The Telegraph,* 11 August 2008, accessed 27 July 2018, https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.
[63] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired,* 11 March 2014, accessed 28 March 2019, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[64] Josh Fruhlinger, "What is Stuxnet, Who Created it and how does it work?" *CSO,* 22 August 2017, accessed 28 March 2019, https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.
[65] Fruhlinger, "What is Stuxnet, Who Created it and how does it work?"
[66] Solis, *The Law of Armed Conflict: International Humanitarian Law in War (2nd Edition),* p. 706.
[67] Heather Harrison Dinniss, *Cyberwarfare and the Laws of War,* (Cambridge: Cambridge University Press, 2012), p. 38.
[68] Dinniss, *Cyberwarfare and the Laws of War,* p. 38.

January 2010.[69] Security cameras installed by IAEA revealed that staff at Iranian nuclear facilities were "feverishly" attempting to fix widespread damage in the summer of 2009 after Stuxnet was apparently first introduced to the facilities.[70] While it is unknown how extensive was the damage , it is known that Iran was forced to replace roughly one thousand centrifuges in a short span.[71] This number of centrifuges is estimated to be equivalent to about one-fifth of Iran's total nuclear centrifuges.[72] Although this is a significant portion of Iran's centrifuges, the overall impact on Iran's enrichment program was relatively minor as Iranian facilities were able to recover functionality in a short span of time.[73] In total, Iran stated in 2010 that roughly 30,000 of its industrial computer systems had been infected with the Stuxnet Virus.[74]

2.21 Aftermath of the Stuxnet Virus

The discovery of the Stuxnet Virus in 2010 was an important milestone because it marked the first documented case of a cyber weapon being deployed with the specific intent of causing kinetic damage to physical systems. The Stuxnet case also made it clear how cyber weapons could be deployed to damage and destroy key nodes within a nation's critical national infrastructure. Since the development of Iran's nuclear program was an important national objective, Stuxnet had the potential to fatally undermine the long-term goals of the Iranian regime.[75] However, the Stuxnet Virus was ultimately unable to seriously impede Iran's nuclear program, and Iran was able to increase its output of enriched uranium after the Stuxnet attack.[76]

[69] Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon."
[70] Kim Zetter, "Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran," *Wired,* 16 February 2011, accessed 28 March 2019, https://www.wired.com/2011/02/isis-report-stuxnet/.
[71] Dinniss, p. 38.
[72] Solis, p. 707.
[73] Ibid., p. 708.
[74] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," *Journal of Computer & Information Law-Fall* 29, 1 (2011): p. 5.
[75] John Richardson, "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," p. 4.
[76] Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* 1, 1 (2015): p. 62.

Despite this, the authors of the *Tallinn Manual* were unanimous in their determination that the damage caused by the Stuxnet Virus should be considered a "use of force."[77] Some experts even believed that the scale and effects of the Stuxnet Virus were sufficient to qualify it as an "armed attack."[78] This determination by some of the authors of the *Tallinn Manual* is significant because it indicates that there is a capacity for hybrid cyber operations to meet the criteria necessary for classification as an "armed attack," and therefore, fulfill the first requirement allowing for a legal use of force in self-defence. However, like in the case of the DDoS attacks on Georgia, attribution for the Stuxnet Virus could not be conclusively shown despite strong indications as to who might be responsible.

Although Iran has acknowledged that it was the victim of "electronic war", it remains unclear as to who orchestrated and carried out the Stuxnet operation.[79] The states of Israel and the United States are generally accepted as the most likely culprits of the attack.[80] They are suspected for political reasons and because the sophistication of the Stuxnet Virus was such that only a few governments would have had the resources necessary to construct and deploy the virus.[81] However, neither these political motivations, nor the sophistication of the cyber operation are sufficient to conclusively prove the case against either Israel and/or the United States.

Indeed, most of the evidence that indicates that Israel and the United States carried out the Stuxnet operation has no legal probative value or is circumstantial at best. For instance, a 2012 article in the New York Times claimed that the Stuxnet Virus was a joint American and Israeli effort codenamed "Olympic Games."[82] Following the release of this article, many other news sources began to attribute the Stuxnet operation to Israel and the US. It became generally accepted public knowledge that they were

[77] Schmitt, rule 71, para 10.
[78] Ibid.
[79] Dinniss, p. 57.
[80] Solis, p. 679.
[81] Buchanan and Rid, "Attributing Cyber Attacks," p. 22.
[82] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times,* 1 June 2012, accessed 10 April 2019, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

responsible for the operation.[83] However, the ICJ noted in the *Nicaragua Case*, "widespread reports of facts may prove on closer inspection to derive from a single source, and such reports, however numerous, will in such case have no greater value as evidence than a single source."[84]

Furthermore, it was not clear where the author of the original New York Times article garnered the information that was necessary to attribute the Stuxnet operation to Israel and the United States. Rather, the article states that the "account of the American and Israeli efforts to undermine the Iranian nuclear program is based on interviews… with current and former American, European and Israeli officials involved with the program."[85] Nowhere does the author of the New York Times article specifically state who these individuals were. This is important because, in the ICJ's judgment regarding the *Democratic Republic of the Congo v. Uganda,* the truth of the case could not be "established by extracts from a few newspapers, or magazine articles, which rely on a single source; on an interested source, or give no sources at all."[86] Consequently, because no specific sources are cited in the New York Times article, the information provided in the article cannot be considered as having the probative value necessary to prove attribution.

Another piece of evidence pointing to possible Israeli involvement in the Stuxnet operation was the presence of certain idiosyncrasies within the code of the virus. Within the code was the marker "19790509," which may be a reference to the 9 May 1979 execution of a Jewish-Iranian businessman in Iran.[87] Additionally, there seemed to be a string of code that was based upon religious references significant to the Jewish people.[88] However, the mere presence of these idiosyncratic pieces of code is not

[83] Roscini, ""Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," p. 262.
[84] International Court of Justice, ""Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)," para 62.
[85] Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran."
[86] International Court of Justice, *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda,* Judgment, 19 December 2005, para 68.
[87] Gregg Keizer, "Stuxnet Code Hints at Possible Israeli Origin, Researchers Say," *Computerworld,* 30 September 2010, accessed 10 April 2019, https://www.computerworld.com/article/2515995/stuxnet-code-hints-at-possible-israeli-origin--researchers-say.html.
[88] Aguirre *et al, Stateless Attribution: Toward International Accountability in Cyberspace,* p. 11.

sufficient to prove Israeli involvement in the incident. In fact, the cybersecurity experts that found the idiosyncratic code were wary to posit attribution based upon this evidence because adding pieces of code that imply attribution to a specific actor is a common method of spoofing used in cyber operations to mislead investigators.[89] As such, the sections of the Stuxnet code that potentially indicate Israeli involvement by no means conclusively show that Israel was responsible for the Stuxnet operation.

In this way, despite the public indictments of the Israeli and American governments and the technical evidence potentially linking Israel to the virus, these pieces of evidence are ultimately insufficient for conclusively showing that either Israel and/or the United States were responsible for the Stuxnet operation. Furthermore, the official statement from both the Israeli and American governments is to neither confirm nor deny involvement in the Stuxnet operation. .[90] Consequently, as no definitive evidence could be found, and neither Israel nor the United States officially accepted responsibility for the virus, attribution for the Stuxnet operation remains inconclusive.

2.3 The Growing Threat of Hybrid Cyber Operations

Following the EU's fact-finding mission in the Russo-Georgian War in 2008, the official report noted that "the nature of defence against cyber attacks at this stage of its development means that such attacks are easy to carry out, but difficult to prevent, and to attribute to a source." [91] A decade later, these findings remain relevant as there have not been any significant developments in international law designed to deal with the threat of hybrid cyber operations. As such, hybrid cyber operations remain extremely difficult to deter. To illustrate this point, Ukraine was the victim of approximately 6500 cyber operations in only a two-month period in 2016. [92] Adding to the growing frequency of hybrid cyber operations is the fact that they are relatively inexpensive to

[89] Aguirre *et al,* p. 12; Keizer, "Stuxnet Code Hints at Possible Israeli Origin, Researchers Say."
[90] Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," p. 262.
[91] Council of the European Union, *Independent International Fact-Finding Mission on the Conflict in Georgia: Volume II,* p. 219.
[92] Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired,* 20 June 2017, accessed 20 February 2019, https://www.wired.com/story/russian-hackers-attack-ukraine/.

undertake. For instance, it is estimated that the cost of the entire cyber operation launched against Georgia was less expensive than the cost of replacing a single tank tread.[93]

Equally concerning is the growing sophistication of cyber weapons technology. When the Stuxnet Virus was discovered in 2010, it was a cyber weapon "unlike any other virus or worm that came before."[94] However, in 2015 and 2016, Ukraine's power grid suffered a debilitating cyberattack from a virus that was "purpose-built to disrupt physical systems" in a manner similar to the Stuxnet operation.[95] This virus codenamed "Crash Override" targeted the Ukrainian electrical grid, which resulted in power loss for nearly 200,000 Ukrainians.[96] The rapid pace of cyber weapons development can be seen in this attack when one considers that the 2015 cyber operation required approximately 20 people to attack three Ukrainian energy companies, while those same 20 people could target ten to fifteen sites by 2016.[97] Furthermore, the vulnerabilities exploited by the "Crash Override" virus were not unique to the Ukrainian electrical grid, as experts believe that these vulnerabilities are present within other types of systems critical national worldwide, such as water treatment plants.[98]

The cyber operations against the Ukrainian electrical grid also make it clear that determining conclusive cyber attribution remains an intractable problem. Although the Russian state has been widely suspected of being responsible for the operations against the Ukrainian electrical grid, conclusive state attribution has not been shown.[99] Rather, for these operations attribution has been linked to a Russian hacking group known as

[93] Markoff, "Before the Gunfire, Cyberattacks."
[94] Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon."
[95] Andy Greenberg, "'Crash Override:' The Malware That Took Down a Power Grid," *Wired*, 12 June 2017, accessed 10 April 2019, https://www.wired.com/story/crash-override-malware/.
[96] Donghui Park, Julia Summers and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," *The Henry Jackson School of International Studies (University of Washington)*, 11 October 2017, accessed 21 February 2019. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn15.
[97] Greenberg, "'Crash Override:' The Malware That Took Down a Power Grid."
[98] Ibid.
[99] Park *et al.*, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks."

"Sandworm."[100] Although many of the hacking activities undertaken by "Sandworm" seem to align with Russian state interests, it remains unclear how much control the Russian state has over this hacking group.[101] As such, it cannot be determined whether the Russia state bears responsibility for the attacks on the Ukrainian power grid, or whether these attacks were the responsibility of cyber criminals alone.[102]

In summary, hybrid cyber operations are being launched with growing frequency and sophistication. At present, there does not seem to be any way to deter hybrid cyber operations from a technical standpoint nor within the existing framework of international law. Even the most technologically advanced and militarily powerful nations in the world seem incapable of deterring cyberattacks. NATO Secretary General Jens Stoltenberg has even publicly stated that "NATO is attacked every single day."[103] Furthermore, it is estimated that roughly three percent of cyberattacks are so complex that they are impossible to stop.[104] Consequently, the manner in which hybrid cyber operations are able to exploit the international law regulating the resort to the use of force in self-defence will likely become more problematic in the future.

Concluding Remarks

Hybrid warfare has emerged as an increasingly difficult challenge for existing international law. Nowhere is this more apparent than in the use of hybrid cyber operations. From a theoretical standpoint, hybrid cyber operations pose a two-pronged dilemma for the international law related to the use of force in the context of self-defence. This dilemma stems from the difficulties associated with establishing that a

[100] Jim Finkle, "U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage," *Reuters,* 8 January 2016, accessed 10 April 2019, https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108.
[101] Aguirre *et al,* p. 8.
[102] Aguirre *et al,* p. 8; & Park *et al.,* "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks."
[103] Jens Stoltenberg, "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference," *NATO,* 15 May 2018, accessed 10 April 2019, https://www.nato.int/cps/en/natohq/opinions_154462.htm.
[104] Myriam Dunn Cavelty, "Cyber-Security," *Contemporary Security Studies 4th Edition,* edited by Alan Collins, (Oxford: Oxford University Press, 2016), p. 404.

cyber operation has risen to the level of an "armed attack" and the near impossibility of conclusively establishing cyber attribution. Without these two requirements, victims of hybrid cyber operations cannot use force in self-defence without committing an internationally wrongful act. In this way, the use of hybrid cyber operations significantly undermines the traditional deterrent value of conventional military power.

As the case studies of Georgia and Stuxnet make clear, the real-world issues associated with hybrid cyber operations are as problematic as the theoretical issues. In the case of the DDoS attacks against Georgia, these cyber operations did not meet the scale and effects necessary for classification as an "armed attack." Moreover, while the authors of the *Tallinn Manual* were unanimous that the Stuxnet virus constituted a "use of force", they were not unanimous that Stuxnet reached the threshold of an "armed attack." Importantly, in neither the case of Georgia nor Stuxnet could attribution be conclusively shown. As such, neither Georgia or Iran could legally use force in the context of self-defence against the likely perpetrators of the hybrid cyber operations.

Looking to the future, hybrid cyber operations are likely to play an increasingly frequent and important role in international disputes between states. This becomes problematic when one considers the seeming inability of international law to effectively regulate this unconventional means of warfare. While interpreting international law from a legal positivist perspective is perhaps the best way to reconcile the core principles of the LOAC with cyberspace, its stringent application of the law makes it ill-suited to regulate hybrid cyber operations. As a result, nations that wish to pursue hybrid cyber operations as a strategic policy can do so from a position of relative safety as international law is seemingly powerless to deter such actions.

Bibliography

Aguirre, Jair, Benjamin Bourdreaux, Michael S. Chase, John S. Davis II, Geoffrey McGovern, Cordaye Ogletree, Johnathan William Welburn. *Stateless Attribution: Toward International Accountability in Cyberspace.* Santa Monica: RAND Corporation, 2017.

British Broadcasting Corporation. "Georgia 'started unjustified war," *BBC News (Online).* 30 September 2009. Accessed 18 February 2019. http://news.bbc.co.uk/2/hi/europe/8281990.stm.

---."South Ossetia Profile," *BBC News (Online).* 21 April 2016. Accessed 27 March 2019. https://www.bbc.com/news/world-europe-18269210

Breithaupt, Jim and Mark S. Merkow. *Information Security: Principles and Practices 2nd Edition.* Indianapolis: Pearson Education, 2014.

Buchanan, Ben and Thomas Rid. "Attributing Cyber Attacks," *The Journal of Strategic Studies* 38, No. 1-2, 4-37.

Cavelty, Myriam Dunn. "Cyber-Security," *Contemporary Security Studies 4th Edition.* Edited by Alan Collins. Oxford: Oxford University Press, 2016. pp. 400-415.

Charter of the United Nations. "Chapter I: Purposes and Principles." Accessed 6 April 2019. http://legal.un.org/repertory/art2.shtml.

---. "Chapter VII: Action With Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," Accessed 9 April 2019. http://www.un.org/en/sections/un-charter/chapter-vii/index.html, art. 51.

CNN. "2008 Georgia Russia Conflict Fast Facts," *CNN.* 3 April 2018. Accessed 27 March 2019. https://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/index.html.

Council of the European Union. *Independent International Fact-Finding Mission on the Conflict in Georgia: Volume I.* Brussels: European Union, 2009.

Council of the European Union, *Independent International Fact-Finding Mission on the Conflictin Georgia: Volume II.* Brussels: European Union, 2009.

Dev, Priyanka R. "Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for a Formal U.N. Response," *Texas International Law Journal* 51, 2 (2015): pp. 381-401.

Dinniss, Heather Harrison. *Cyberwarfare and the Laws of War,* Cambridge: Cambridge University Press, 2012.

Dyment, Jan. "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence," *Security Intelligence,* 28 December 2018. https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/.

Finkle, Jim. "U.S. Firm Blames Russian 'Sandworm' Hackers for Ukraine Outage," *Reuters.* 8 January 2016. Accessed 10 April 2019. https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108.

Focarelli, Carlo. "Self-defence in cyberspace," *International Law and Cyberspace,* edited by Russell Buchan and Nicolas Tsagourias. North Hampton: Edward Elgar Publishing Inc., 2015, pp. 255- 283.

Fruhlinger, Josh. "What is Stuxnet, Who Created it and how does it work?" *CSO.* 22 August 2017. Accessed 28 March 2019. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html.

Green, Leslie. "Legal Positivism," *The Stanford Encyclopedia of Philosophy.* Spring 2018 Edition. Edited by Edward N. Zalta. Accessed 6 March 2019. https://plato.stanford.edu/entries/legal-positivism/#4.

Greenberg, Andy. "'Crash Override:' The Malware That Took Down a Power Grid," *Wired.* 12 June 2017. Accessed 10 April 2019. https://www.wired.com/story/crash-override-malware/.

---. "How an Entire Nation Became Russia's Test Lab for Cyberwar," *Wired,* 20 June 2017. Accessed 20 February 2019. https://www.wired.com/story/russian-hackers-attack-ukraine/.

Goryashko, Sergei. "South Ossetia: Russia Pushes Roots Deeper into Georgian Land," *BBC,* 8 August 2018. Accessed 27 March 2018. https://www.bbc.com/news/world-europe-45100160.

Hay, Lily. "Hacker Lexicon: What is the Attribution Problem?" *Wired,* 24 December 2016. Accessed 23 March 2019. https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/.

Hill, Stephen. "Briefing on NATO and International Law." Presentation, Simon Fraser University NATO Field School, Brussels, 26 June 2018.

Hobbes, Thomas. *De Cive.* Copenhagen: Titan Read, 2015.

International Court of Justice. *The Corfu Channel Case (Merits),* Judgments. Merits. 9 April 1949.

---. "Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)," Judgement, 27 June 1986,

---. *Legality of the Threat or Use of Nuclear Weapons.* Advisory Opinion. 8 July 1996. ICJ Reports 1996.

---. *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda,* Judgment. 19 December 2005.

Keizer, Gregg. "Stuxnet Code Hints at Possible Israeli Origin, Researchers Say," *Computerworld.* 30 September 2010. Accessed 10 April 2019. https://www.computerworld.com/article/2515995/stuxnet-code-hints-at-possible-israeli-origin--researchers-say.html.

Korns, Stephen and Joshua Kastenberg. "Georgia's Cyber Left Hook," *Parameters* 38. No. 4. Winter 2008/2009, pp. 60-76.

Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat (Online),* 31 July 2017, accessed 2 August 2018. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Lindsay, Jon R. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack," *Journal of Cybersecurity* 1. 1 (2015): p. 53-67.

Markoff, John. "Before the Gunfire, Cyberattacks," *The New York Times.* 12 August 2008. Accessed 28 March 2019. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Park, Donghui, Julia Summers and Michael Walstrom. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," *The Henry Jackson School of International Studies (University of Washington).* 11 October 2017. Accessed 21 February 2019. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn15.

Richardson, John. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield," *Journal of Computer & Information Law-Fall* 29, 1 (2011): pp. 1-28.

Roscini, Marco. "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations," *Texas International Law Journal* 50, 2 (2015).

Ruiz Palmer, Diego A. "Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons," *NATO Defense College Research Division,* No. 120, October 2015, pp. 1-12.

Rusnakova, Sona. "Russian New Art of Hybrid Warfare in Ukraine," *Slovak Journal of Political Sciences* 17, 3-4 (2017): pp. 343-380.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times.* 1 June 2012. Accessed 10 April 2019. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

Schmitt, Michael N. *Tallinn Manual 2.0: On The International Law Applicable to Cyber Operations.* New York: Cambridge University Press, 2017.

Slack, Chelsey. "Briefing on NATO and Cybersecurity." Presentation, Simon Fraser University NATO Field School, Brussels, 28 June 2018.

Solis, Gary D. *The Law of Armed Conflict: International Humanitarian Law in War (2nd Edition).* New York: Cambridge University Press, 2016.

Stoltenberg, Jens. "Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference," *NATO.* 15 May 2018. Accessed 10 April 2019. https://www.nato.int/cps/en/natohq/opinions_154462.htm.

Swaine, Jon. "Georgia: Russia 'conducting cyber war'." *The Telegraph.* 11 August 2008, accessed 8 February 2019. https://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html.

Symantec Expert Perspectives. "The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks," *Symantec Corp.* 3 October 2018. https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks.

Tsagourias, Nicolas. "Cyber Attacks, Self-Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, 2 (2012): pp. 229-244.

Turns, David. "Cyber war and the law of neutrality." *International Law and Cyberspace.* Edited by Russell Buchan and Nicolas Tsagourias. North Hampton: Edward Elgar Publishing Inc., 2015. pp. 380-402.

United Nations General Assembly. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 24 June 2013. UN Doc A/68/98.

---. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." 22 July 2015, UN Doc A/70/174.

White, Sarah P. "Understanding Cyberwarfare: Lessons from the Russia-Georgia War," *Modern War Institute.* 20 March, 2018. Accessed 27 March 2019. https://mwi.usma.edu/understanding-cyberwarfare-lessons-russia-georgia-war/.

Zetter, Kim. "Surveillance Footage and Code Clues Indicate Stuxnet Hit Iran," *Wired.* 16 February 2011. Accessed 28 March 2019. https://www.wired.com/2011/02/isis-report-stuxnet/.

---."An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired.* 11 March 2014. Accessed 28 March 2019. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Ziolkowski, Katharina. "NATO and cyber defence," *International Law and Cyberspace,* edited by Russell Buchan and Nicolas Tsagourias. North Hampton: Edward Elgar Publishing Inc., 2015, pp. 426-445.