National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE ETHICS OF CYBER ATTACK: ARE OFFENSIVE CYBER OPERATIONS AN ETHICAL OPTION IN MODERN WARFARE?

Major Jeremy Wigmore

JCSP 46 DL	PCEMI 46 AD
Solo Flight	**Solo Flight**
Disclaimer	**Avertissement**
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.	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.
© 2021 Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence.	© 2021 Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale..

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 DL – PCEMI 46 AD
2019 – 2021

SOLO FLIGHT

THE ETHICS OF CYBER ATTACK: ARE OFFENSIVE CYBER OPERATIONS AN ETHICAL OPTION IN MODERN WARFARE?

By Major Jeremy Wigmore

“This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l’une des exigences du cours. L’étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l’auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l’opinion d’un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

THE ETHICS OF CYBER ATTACK: ARE OFFENSIVE CYBER OPERATIONS AN ETHICAL OPTION IN MODERN WARFARE?

INTRODUCTION

The technological advancements of the Information Age have transformed and improved nearly every facet of modern life. Social wellness has been enhanced through unprecedented digital access to information, education, people, entertainment, and virtual communities for the globally low cost of internet access. Economic advancements from the Information Age have helped to cut the global extreme poverty rate by two-thirds in the last three decades, as more than one billion people in Asia alone have been lifted out of abject poverty.[1] Indeed, the networks providing the backbone of the Information Age have had a profound effect on the wellbeing of billions of people.

Despite the countless opportunities provided by these networked systems, new threats have emerged which seek to exploit network vulnerabilities for a variety of purposes. From cyber-criminals seeking financial gain, to "hacktivists" who break into networks for political or social reasons, to actors of nation-states who pursue national ends, the interconnected nature of cyberspace provides novel ways for actors to pursue their goals.[2] Activities in cyberspace have become an indelible part of contemporary military operations for cyber-empowered and modern militaries, as well as lower-tech forces; resultingly, a debate has emerged on the ethics of offensive military activities in the interconnected domain of cyberspace.[3]

[1] Max Roser and Esteban Ortiz-Ospina, "Global Extreme Poverty", accessed on 29 May 2021, https://ourworldindata.org/extreme-poverty.

[2] Georg Thomas, "On the offensive: is 'hacking back' ethical?", *Higher Degree by Research Symposium*, October 2017, https://www.researchgate.net/publication/320445115_On_the_offensive_is_%27hacking_back%27_ethical.

[3] Michael Schmitt, "The Law of Cyber Targeting", *Naval War College Review,* 68, 2 (Spring 2015), 11.

Although offensive military cyber operations have the potential to both enhance and threaten the ethical conduct of modern conflict, this paper will argue that if carefully controlled, responsible States could ethically pursue offensive cyber operations. The first section of this paper will introduce key terminology and explore the unique characteristics of the cyber domain. The second section will identify several ways offensive cyber operations could enhance the ethical outcomes of warfare. In the third section, an opposing view will consider how offensive cyber operations could jeopardize ethical outcomes in modern conflict. The final section will suggest considerations and parameters for the ethical conduct of offensive cyber operations. Though the detailed technical elements of cyber capabilities are relevant to this discussion, they are beyond the scope of this paper.

The Cyber Domain – Key Terminology and Unique Characteristics

Cyberspace has been defined as: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[4] States are able to exert *cyber power* to promote security and other national interests in and through cyberspace through offensive and defensive measures.[5] *Offensive cyber operations* – also known as *cyber attack* – refer to "…deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or

[4] Department of Defense, US Joint Publication 3-12, *Cyberspace Operations*, (Washington, DC: US Joint Chiefs of Staff, 8 June 2018), GL-4.

[5] David Lonsdale, "The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios," *Journal of Military Ethics*, No. 1, Vol 19, 2020, 23.

transiting these systems or networks."[6] Cyber attacks are executed through the use of cyber weapons known as *malware* – malicious software that has been specifically designed to damage, disrupt, or gain unauthorized access to a computer system. *Defensive cyber operations* are operations to preserve cyberspace capabilities and protect data, networks, and devices from ongoing or imminent malicious cyberspace activity.[7] A key element of cyberspace and the operations conducted within, is that unlike the traditional maritime, land, and aerospace domains, the cyber domain is not defined by physical locations; instead, much of the cyber domain is uniquely non-physical.[8]

The uniqueness of cyberspace is further illustrated when one considers the concepts around which the global order is organized. The centuries-old Westphalian concept of sovereignty, for example, is key to defining the concepts of territorial integrity and non-intervention which are codified in the United Nations Charter.[9] While straightforward when viewed through the lens of traditional domains – e.g. sovereignty is breached when adversary forces cross well-defined physical boundaries – there is no internationally accepted concept of cyberspace sovereignty. Moreover, for nations to project significant power in the land, maritime, and aerospace domains, the costs of operating with consequence are several orders of magnitude higher than the relatively

[6] Christopher Bailey, "Cyber Civilians as Combatants," *International and Comparative Law Journal* 8 no. 1 (2017), 8.

[7] Department of Defense, US Joint Publication 3-12, *Cyberspace Operations*, (Washington, DC: US Joint Chiefs of Staff, 8 June 2018), GL-4.

[8] The Canadian Armed Forces' cyberspace model describes three layers of cyberspace: the physical layer consisting of the physical devices and hardware; the logical layer, which consists of data and digital information; and the cyber-persona layer, which are the virtual identities of people within cyberspace. For more, see Canadian Forces Warfare Centre, *Joint Doctrine Note - Cyber Operations* (Ottawa: Department of National Defence, 2017).

[9] United Nations, "Article 2 (4) – Prohibition of threat or use of force in international relations", accessed on 30 May 2021, https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter#rel2.

low cost of entry to the cyber domain.[10] Several authors are working to continue the refinement of the concept of cyber sovereignty; however, this topic will not be discussed further in this paper.[11]

The unique characteristics of the cyber domain provide important context for the examination of ethical considerations of offensive cyber operations. In the next section, these operations will be examined to demonstrate the opportunities for enhanced ethical outcomes in conflict.

The Ethical Case "For" Offensive Cyber Operations

The argument for offensive cyber operations often describes the use of cyber weapons as a less destructive alternative to conventional or kinetic weapons; consequently, some advocates promote cyberwar as an ideal form of war.[12] As cyber weapons are generally employed against computers, networks, and data, the consequences of cyber attack can differ vastly from traditional weapons systems, especially in terms of limiting collateral damage.[13]

As with kinetic weapons, cyber weapons can cause physical damage to computer systems and other networked systems.[14] In the famous Stuxnet cyber attack, 984 centrifuges in Iran's Natanz uranium enrichment facility were deliberately destroyed through the use of malware, which ultimately delayed the advancement of Iran's nuclear

[10] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace", *Orbis* 61, 3 (Summer 2017), 381, 382.

[11] For further discussion of cyber sovereignty, see Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0*, (Cambridge: Cambridge University Press, 2017), or Lonsdale, "The Ethics of Cyber Attack…", 30.

[12] Ryan Jenkins, "Cyberwarfare as Ideal War", in *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, (Oxford: Oxford University Press, 2016), 89.

[13] Edward Barrett, "On the Relationship Between the Ethics and Law of War: Cyber Operations and Sublethal Harm", *Ethics & International Affairs* 31, no. 4 (2017), 470.

[14] *Ibid.*

program.[15] To achieve comparable effects through kinetic weapons, powerful munitions would have been required to strike the underground facility, and the risk of collateral damage would have been comparatively higher.[16] Stuxnet served as an ethical cyber weapon that was able to deliver a precise strike against Iran's nuclear capability without producing a single fatality or injury.[17]

In contrast to the lasting effects of kinetic weapons, the effects of specific cyber attacks (such as distributed-denial-of-service (DDoS) or ransomware) can be immediately reversible, leaving no signs that the attack occurred.[18] This unique capacity for reversible effects represents a potent tool of policy, as belligerents could impose temporary losses of functionality or capability against their adversaries, without the long-term consequences of violence.[19] While the losses of services such as electricity could have a powerful impact on military operations and civilian populations in a conflict zone, service interruptions from reversible offensive cyber actions are likely to be restored faster than if the critical electrical infrastructure was significantly damaged through kinetic action. From the ethical perspective, minimizing the enduring consequences of conflict is a significant advantage of offensive cyber operations.

[15] McAfee Security, "What Is Stuxnet?", accessed on 30 May 2021, https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware/what-is-stuxnet.html.

[16] Frank Gardner, "Why Iran's nuclear facilities are still vulnerable to attack", *BBC*, 19 January 2021, https://www.bbc.com/news/world-middle-east-55271429.

[17] P.W. Singer, "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons", *Case Western Reserve Journal of International Law* 47, No. 1 (2015), 85.

[18] A DDoS attack uses a large network of computers (a botnet) to simultaneously and persistently attempt to connect to a server, overwhelming the server and causing the system to crash. A ransomware attack infects a target computer with malware which holds the user's data at ransom - usually by encrypting all data on the device and rendering it inaccessible to its user. To recover the data, the attacker typically demands a ransom be paid via cryptocurrency in exchange for the encryption key. In both of these instances, the users' systems are rendered non-functional; however, they are not physically damaged. At the attacker's discretion, the botnet can be commanded to cease a DDoS attack or the ransomware encryption key can be provided, allowing the user to recover their systems without further compromise in functionality.

[19] Lonsdale, "The Ethics of Cyber Attack…", 28.

The policy and strategic opportunities presented by non-violent offensive cyber operations are potentially profound. As David Londsdale concluded: "Without the consequences of violence and destruction, cyber attack could be equated more diplomatic and economic sanctions, rather than considered a form of war."[20] For technologically advanced belligerents, offensive cyber operations present a means to bring about favorable outcomes short of costly, labour and resource intensive, conventional military operations.[21] By using offensive cyber operations in lieu of force-on-force conventional engagements, the ethical outcomes of the conflict can be enhanced as not only are the consequences suffered by non-combatants diminished, but so too are the casualties and consequences born by belligerents *on all sides* of the conflict.

As an offensive cyber weapon, Stuxnet was designed to meticulously strike precise strategic targets and its employment produced no collateral damage, earning it the title of the world's first "purely ethical weapon".[22] When compared against the conventional options to achieve a belligerent's desired effects, offensive cyber operations offer the clear ethical advantages of being uniquely able to minimize long-term consequences as well as universally lower human casualties within the conflict. Despite the ability of offensive cyber operations to improve the ethical outcomes of conflict, their use also introduces unique ethical challenges.

The Ethical Case "Against" Offensive Cyber Operations

Two central arguments lie at the heart of the ethical debate against offensive cyber operations. The first argument contends that offensive cyber operations may violate

[20] Lonsdale, "The Ethics of Cyber Attack…", 25.
[21] Bailey, "Cyber Civilians as Combatants", 9.
[22] George. R. Lucas, "Emerging Norms for Cyberwarfare", in *Binary Bullets: The Ethics of Cyberwarfare*, edited by Allhoff, Henschke, and Strawser, (Oxford: Oxford University Press, 2016), 28.

specific foundational principles of distinction and proportionality in international humanitarian law. The second argument is that due to the stealthy nature of cyber operations, misidentification or uncertainty of the attacker may invite escalation into wider or more intense conflict.

Additional Protocol I to the Geneva Conventions establishes international humanitarian laws to protect civilian populations in conflict. One of the foundational principles is the requirement for *distinction* between military and civilian personnel and objects. Indiscriminate attacks – attacks which are not directed at a specific military objective or using weapons which create uncontrollable effects – are prohibited under Article 51 of Additional Protocol I.[23] In conventional operations, the quantity of dual-use objects which are used by both militaries and civilians – and can lawfully be attacked – is comparatively lower than operations conducted in the cyber domain. As Michael Schmitt describes: "The harsh reality of twenty-first-century military cyber activity is that the heavy reliance on civilian products and infrastructure dramatically expands the universe of targetable objects, including systems on which important civilian functions rely."[24] Some experts have argued this broad expansion of targets violates the traditional understanding of the principle of distinction, as dual-use targets in the cyber domain could result in persons who, through the conventional lens would not be considered to be directly participating in hostilities – like employees at Facebook, Google, Microsoft, or Apple – becoming legitimate targets of war.[25]

[23] International Committee of the Red Cross, *Protocols Additional to the Geneva Conventions of 12 August 1949*, (Geneva: ICRC, May 2010), 37.

[24] Schmitt, "The Law of Cyber Targeting", 19.

[25] Lonsdale, "The Ethics of Cyber Attack…", 26.

A second ethical concern relating to the principle of distinction arises from the extent to which cyber weapons can be controlled once deployed. As cyber weapons are often designed to spread through computer networks, a cyber weapon deployed against a legitimate military target may escape from its intended network and spread across any connected civilian systems, potentially causing indiscriminate and uncontrollable effects.[26] Moreover, if the cyber weapon's effects cannot be monitored or deactivated at the end of hostilities, then the malware would violate the principle of *proportionality*, and would continue to pose risks like a digital landmine.[27] A recent, large-scale cyber attack demonstrated the consequences of an indiscriminate and disproportionate cyber weapon.

One of the worst cyber attacks in history occurred in 2017, when a piece of malware named NotPetya began infecting and encrypting millions of computers around the world and resulted in damages exceeding ten billion dollars. Assessed as being a state-developed Russian military cyber weapon deployed in the undeclared war between Russia and Ukraine, the software rapidly spread beyond the Ukrainian targets and moved into a wide range of civilian networks around the world. NotPetya destroyed the networks of major corporations like the Maersk shipping company and pharmaceutical giant Merck, and disrupted operations in American hospitals, Tasmanian factories, and the Russian state oil company, Rosneft.[28] NotPetya demonstrated that potent cyber weapons, if not sufficiently controlled, can produce widespread and indiscriminate effects which are unethical and in violation of international humanitarian law.

[26] Schmitt, "The Law of Cyber Targeting", 23.

[27] Lonsdale, "The Ethics of Cyber Attack…", 28.

[28] Aparna Banerhea, "NotPetya: How a Russian malware created the world's worst cyberattack ever", *Business Standard*, 27 August 2018, https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html.

Operations in the cyber domain present unique challenges which may result in unethical escalation of conflict. Within the conventional domains, it is comparatively easy to determine when an attack is occurring in physical space as well as the identity of the attacker; however, due to the unique nature of cyberspace, determining an attack is occurring or has occurred and identifying the attacker can be far more difficult.[29] In the cyber domain, connections are extensively routed through the Internet, transiting any number of networks and servers throughout the world: a piece of malware launched by an attacker in a particular location is likely to be routed through several countries – often without these states' knowledge – on its way to the target.[30] Attackers often employ techniques to deliberately obfuscate the origins of the attack, further complicating the resultant forensic evaluation – which is notoriously slow and rarely reveals the identity of the attacker with absolute certainty.[31]

Compounding the problem of inaccurate attribution is the wide variety of actors with disparate motivations for launching an attack coupled with the apparent similarities of attacks from different actors: it may be impossible to immediately discern a DDoS cyber attack targeting a government agency launched by a foreign state motivated by strategic goals from a domestic 'hacktivist' organization seeking social change. NotPetya was designed to appear to be ransomware – the malware of choice for cyber criminals seeking financial gains – but forensic analysis revealed the fake payment information was randomly generated and there was no encryption key available to users to recover their

[29] Anatonia Chayes, "Cyber Attacks and Cyber Warfare: Framing the Issues", in *Borderless Wars: Civil Military Disorder and Legal Uncertainty*, (Cambridge: Cambridge University Press, 2015), 132-133.
[30] Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2020*, (Ottawa: Communications Security Establishment, 2020), 23.
[31] Lonsdale, "The Ethics of Cyber Attack…", 27.

data. Analysts assess the malware was disguised as ransomware to conceal its true destructive purposes and divert attribution to cyber criminal organizations instead of the Russian government.[32]

The ethical issues resulting from inaccurate attribution become most apparent as options for response are considered. A false accusation resulting from obfuscated attack transiting through a neutral country could trigger a diplomatic crisis or escalatory retaliation, expanding the scope and consequences of the conflict.[33] In exceptional cases, if authentic state agency cannot be determined, attacked states may opt for more extreme or indiscriminate forms of counterattack through *mutually assured disruption* or a so-called "doomsday virus".[34] Moreover, retaliation from cyber attack is not limited to the cyber domain as a State may choose to respond with conventional means. In the 2018 *Nuclear Posture Review*, the United States declared that in extreme circumstances, the U.S. could consider a nuclear response following a devastating cyber attack on the country.[35] In each of these cases, there is a clear risk of escalation and subsequent risk of unethical outcomes when a defender cannot accurately attribute the origin of a cyber attack.

Offensive cyber operations have the potential to jeopardize the conduct of modern, ethical warfare. Poorly designed cyber weapons which cannot be monitored or controlled invite violations of the principles of distinction and proportionality under international humanitarian law. States who deliberately obfuscate their attacks through

[32] Josh Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now", *CSO Online*, 17 October 2017, https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.
[33] Chayes, "Cyber Attacks and Cyber Warfare…", 143.
[34] Lonsdale, "The Ethics of Cyber Attack…", 27.
[35] Department of Defense, *Nuclear Posture Review*, (Washington, DC: Secretary of Defense, February 2018), 21.

neutral parties increase the global risks for wrongful attribution and the concomitant risks of escalation or expansion of the conflict.

Consideration and Parameters for Ethical Offensive Cyber Operations

Cyber operations are an emerging and revolutionary tool of State power, and the belligerents in future conflicts are unlikely to forego cyber's many advantages.[36] As with many novel technologies in warfare, the internationally accepted norms for employment of cyber operations have not yet been codified. Significant attempts to understand the applicability of extant law to cyber operations have been captured in publications such as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*; however, such studies are academic in nature and are non-binding upon States.[37] Since norms typically emerge through behaviors and then are refined through international discourse, and given there is disagreement between States on what constitutes acceptable behaviour, it is unlikely that global norms for cyber conflicts will be adopted in the near term.[38] This section will focus on how Canada and other nations could ethically pursue offensive cyber operations and shape the evolution of global norms governing the use of cyber weapons.

Comparing the ethical opportunities presented by offensive cyber operations – minimized collateral damage and long-term consequences – against the risks of insufficiently controlled cyber weapons – indiscriminate, disproportionate, or escalatory effects – key considerations and parameters emerge:

[36] Bailey, "Cyber Civilians as Combatants", 9.

[37] The *Tallinn Manual* is an academic study of the applicability of international humanitarian law to conflicts in the cyber domain. The first iteration was published in 2013 with a second version in 2017. A third edition is expected in 2026. For more, see Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0*, (Cambridge: Cambridge University Press, 2017), or https://ccdcoe.org/research/tallinn-manual/.

[38] Fischerkeller and Harknett, "Deterrence is Not a Credible Strategy…", 383.

- First, international humanitarian law requires that belligerents minimize collateral damage. The principle of proportionality obliges States to *precautions-in-attack*, requiring belligerents to consider alternative weapons, tactics, and targets to minimize incidental civilian harm. For a given military objective, if cyber means are reasonably available and expected to produce the least collateral damage without sacrificing the likelihood of operational success, then the attacker must use cyber; failing to do so would violate the law.[39]
- Second, when attacking dual-use targets – e.g. key infrastructure – and to the extent possible, weapons with reversible effects should be considered to minimize the suffering and costs imposed upon civilians post-conflict.
- Third, attackers must take extreme care to design and deploy weapons which are highly discriminate and include sufficient control measures to limit effects beyond their target. Stuxnet provided an excellent example of a highly discriminate weapon: despite the malware escaping the Natanz enrichment facility and infecting civilian systems, it did not cause any damage: "Unless you happen to be running a large array of exactly 984 Siemans centrifuges simultaneously, you have nothing to fear from this worm".[40] Such development will require extensive reconnaissance to understand the target system, as well as features like a 'kill-switch' to enable the attacker to deactivate the weapon on command to comply with the principle of proportionality.

[39] Schmitt, "The Law of Cyber Targeting", 24, 25.
[40] Lonsdale, "The Ethics of Cyber Attack…", 27.

- Fourth, care must be taken to insulate from unnecessary expansion or escalation of conflict. Attribution is likely to remain a challenge in the cyber domain and States are unlikely to advertise their offensive cyber capabilities – especially in situations of grey-zone competition short of conflict. More research will be required in this area to understand how risks of escalation can be managed.

CONCLUSION

Offensive cyber operations have the potential to enhance as well as jeopardize the ethical outcomes of conflict. The deliberate employment of cyber weapons can be used to achieve enhanced ethical outcomes by limiting collateral damage and the long-term consequences of conflict, but their employment must be carefully controlled to insulate against indiscriminate, disproportionate, or escalatory effects.

Cyberspace offers myriad opportunities for actors to pursue their ends; yet, without international standards of conduct, the risks of objectionable outcomes is growing. As the world stage is being reset for a resurgence of great power competition, Canada and her allies have a unique opportunity and responsibility to shape the emerging norms of acceptable conduct in cyberspace.

BIBLIOGRAPHY

Bailey, Christopher. “Cyber Civilians as Combatants”. *International and Comparative Law Journal* 8 no. 1 (2017): 4-22.

Banerhea, Aparna. “NotPetya: How a Russian malware created the world’s worst cyberattack ever”. *Business Standard*. 27 August 2018. https://www.business-standard.com/article/technology/notpetya-how-a-russian-malware-created-the-world-s-worst-cyberattack-ever-118082700261_1.html.

Barrett, Edward. “On the Relationship Between the Ethics and Law of War: Cyber Operations and Sublethal Harm”. *Ethics & International Affairs* 31, no. 4 (2017): 467-477.

Canada. Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2020.* Ottawa: Communications Security Establishment, 2020.

Canada. Canadian Forces Warfare Centre. *Joint Doctrine Note - Cyber Operations.* Ottawa: Department of National Defence, 2017.

Chayes, Anatonia. “Cyber Attacks and Cyber Warfare: Framing the Issues”. In *Borderless Wars: Civil Military Disorder and Legal Uncertainty*, 130-143. Cambridge: Cambridge University Press, 2015.

Fischerkeller, Michael P. and Richard J. Harknett. “Deterrence is Not a Credible Strategy for Cyberspace”. *Orbis* 61, 3 (Summer 2017): 381-393.

Fruhlinger, Josh. “Petya ransomware and NotPetya malware: What you need to know now”. *CSO Online*. 17 October 2017. https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html.

Gardner, Frank. “Why Iran’s nuclear facilities are still vulnerable to attack”. *BBC*. 19 January 2021. https://www.bbc.com/news/world-middle-east-55271429.

International Committee of the Red Cross. *Protocols Additional to the Geneva Conventions of 12 August 1949*. Geneva: ICRC, May 2010.

Jenkins, Ryan. “Cyberwarfare as Ideal War”. In *Binary Bullets: The Ethics of Cyberwarfare*. Edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 89–114. Oxford: Oxford University Press, 2016.

Lonsdale, David. “The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios”. *Journal of Military Ethics*, No. 1, Vol 19 (2020): 20-39.

Lucas, George. R. "Emerging Norms for Cyberwarfare". In *Binary Bullets: The Ethics of Cyberwarfare*. Edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 13-33. Oxford: Oxford University Press, 2016.

McAfee Security. "What Is Stuxnet?". Accessed on 30 May 2021. https://www.mcafee.com/enterprise/en-ca/security-awareness/ransomware/what-is-stuxnet.html.

Roser, Max and Esteban Ortiz-Ospina. "Global Extreme Poverty". Accessed on 29 May 2021. https://ourworldindata.org/extreme-poverty.

Schmitt, Michael. "The Law of Cyber Targeting". *Naval War College Review,* 68, 2 (Spring 2015): 11-29.

—. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

Singer, P.W. "Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons", *Case Western Reserve Journal of International Law* 47, No. 1 (2015): 79-86.

Singer, P.W and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014.

Thomas, George. "On the offensive: is 'hacking back' ethical?". *Higher Degree by Research Symposium*. October 2017. https://www.researchgate.net/publication/320445115_On_the_offensive_is_%27hacking_back%27_ethical.

United Nations. "Article 2 (4) – Prohibition of threat or use of force in international relations". Accessed on 30 May 2021. https://www.un.org/securitycouncil/content/purposes-and-principles-un-chapter-i-un-charter#rel2.

United States. Department of Defense. *Nuclear Posture Review*. Washington, DC: Secretary of Defense, February 2018.

United States. Department of Defense. US Joint Publication 3-12, *Cyberspace Operations*. Washington, DC: US Joint Chiefs of Staff, 8 June 2018.