Mitigating the Human Cost of Modern Conflict: Jus in Bello and Cyberattacks

https://www.e-ir.info/2019/10/05/mitigating-the-human-cost-of-modern-conflict-jus-in-bello-and-cyberattacks/

TORY IGOE, OCT 5 2019

Emerging technology continues to revolutionize all traditional forums for human activity. Known as the Fourth Industrial Revolution,[1] the innovation of this century has been sparked by the ongoing development of artificial intelligence (AI), machine learning, and expansion of cyberspace. Within cyberspace lies unlimited potential to benefit humanity, but falls victim to a security dilemma in which continued economic and military competition is lead by technologically developed stakeholders (Buchanan 2019: 3). Cyberspace now embodies a critical area of debate centered primarily on the modern conflict landscape (Schmitt 2017: 4). On 24 June 2013, the United Nations' (UN) Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications (ICT) in the Context of International Security stated that the UN Charter is applicable within cyberspace (UNGA 2013: 2). This proclamation solidified the notion that cyberspace is the fifth domain for warfare (The Economist Briefing 2010). The Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, finalized in 2017, became the primary source on how sovereignty, state responsibility, human rights, and the law of air, space, and the sea apply to cyberspace (Schmitt 2017: 10). This piece thoroughly documents the relevance of *jus ad bellum[2]* to cyber conflict, but the applicability of *jus in bello[3]* to cyberattacks yields scant scholarship due to its lack of precedent and few available frameworks of direct relation. This paper will, therefore, utilize the publications of the International Committee of the Red Cross (ICRC) in addition to the Tallinn Manual 2.0 to establish the extent to which existing norms and principles of international humanitarian law (IHL) apply to cyberattacks in an active conflict setting.

The Cyber Threat Landscape

In order to demonstrate the human cost and consequent applicability of IHL to cyberattacks, a technical summary must precede a discussion around a weaponized cyberspace. Under a general scope, the European Union Agency for Network and Information Security (ENISA) defines the 'Internet of Things' (IoT) as, "a cyber-physical ecosystem of interconnected systems and actuators, which enable intelligent decision making" (ENISA 2017: 1). Cloud computing serves as the backbone of this system, as cloud computing enables citizens and states alike to store and analyze vast quantities of data in real-time while undersea fiber optic cables serve as the high speed data transmission medium (Routely 2017). Given the enormity of modern data use, companies are exploring the possibility of manufacturing more fiber optic cables in the International Space Station (The Economist Briefing 2018). This symbiotic relationship has transformed civil society, but evokes grave concerns in return. The relationship depends on the preservation of 'grids,' or the generation, transmission, distribution and consequent end use of electricity (US Department of Energy 2014). As personal data, energy utilities, infrastructure, healthcare facilities, transportation, and peoples' homes are interconnected and remotely addressable (World Economic Forum 2019), the security implications include the ability to compromise all of the data underpinning a civil society's day-to-day operations (Deloitte 2019). Therefore, distinguishing the various branches of threats within the cyber threat landscape proves useful to building upon a baseline technical understanding.

Given the ever-evolving nature of cyberspace, new threats materialize almost daily (Knake & Clarke 2012: 5). The most prevalent threats to the modern cyber ecosystem include cyber espionage, cybercrime, cyber-enabled disinformation campaigns and cyberattacks. Within the context of economic and political relations between nation-states, these practices hold a unique sphere within the emergence of modern conflict. Each topic varies in definition

depending on the consulted legal code (Rubenstein 2014), so a generalized definition will be proposed for the purpose of differentiating between branches. Cyber espionage, in short, involves the cyber-enabled theft of government or corporate intellectual property (IP) (Kessler 2017). APT40, a Chinese cyber espionage group, is a primary example, as they target strategically placed states relative to the 'Belt and Road Initiative'[4] (FireEye 2019). Cybercrime is far broader, as the Budapest Convention put forth by the Council of Europe (COE) defines cybercrime as, 'criminal acts that are committed [through] online electronic communication networks and information systems' (Council of Europe 2001: 7). The Silk Road, a dark web marketplace dedicated to trafficking illicit goods (Nimfuehr 2018), serves as the most famous example of an act of cybercrime. Distinctive from the preceding branches, cyber-enabled disinformation campaigns are the modern incarnation of an ancient war tactic. Within the sphere of information geopolitics and propaganda, a cyber-enabled disinformation campaign involves the conscious spreading of false information to influence a specific outcome (Rosenbach & Mansted 2019). The influence campaign spearheaded by the Russian Federation against the United States' 2016 election epitomizes the harm cyber-enabled 'fake news' may yield (Nye 2019). These practices embody some of the greatest hazards to cyber stability, but do not possess the equivocal physical impact day-to-day operations may feel following a cyberattack.

Issued by Rule 30 of the Tallinn Manual 2.0, 'a cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects' (Schmitt 2017: 94). This definition fails to highlight the variances in cyberattacks, but emphasizes the crippling outcome if done effectively. Stemming from its umbrella definition, the most common forms of cyberattacks include denial-of-service (DDoS),[5] man-in-the-middle (MitM),[6] phishing,[7] drive-by attack,[8] password cracking,[9] SQL injection,[10] cross-site scripting (XSS),[11] eavesdropping attack,[12] birthday attack,[13] and malware attacks.[14] This strata of methodologies demonstrate how cyberattacks vary in approach and severity, but may damage civil society across a range of operations.

Independent from severity, all of the previously mentioned attacks can be checked at any point of the 'cyber kill chain.' Published by Lockheed Martin Corporation in 2011 as an intelligence driven defense model, the seven steps of the cyber kill chain – reconnaissance, weaponization, delivery, exploitation, installation, command & control (c2), and actions on objectives – describe the path a cyberattack must take to achieve its ultimate objective (Lockheed Martin Corporation 2019: 3). Governments and private sector entities now understand that stopping adversaries at any point of the seven stages ends the attack in its entirety (Panda Security 2019: 5). Unfortunately, copious forms of cyberattacks – both well-known and those of enhanced complexity – reach their objective successfully. Highlighted by Microsoft Corporation's recent announcement that state actors targeted 10,000 customer accounts in the past year (Burt 2019), the mechanisms in place to protect civilians, states and critical infrastructure fall short. Thus, further analysis into weaponizing cyberspace within a pre-existing conflict sparks alarm.

To preface the discussion of cyberattacks capable of astounding harm, six cyber nation-state powers exist within the modern cyber threat landscape. These states include the United States (US), the United Kingdom (UK), Russia, China, North Korea, and Israel (Vavra 2017). Despite varying cyber capabilities, each embrace cyberattacks as a method of statecraft due to the dependence of civil society on an electrical grid, the symbiotic relationship between IoT and cloud computing, in addition to the existence of billions of mobile devices. Thus, cyber offensive capabilities make a lucrative military strategy. An example of a targeted cyberattack on critical infrastructure undertaken by a state against another state occurred on 23 December 2015. Presumed Russian hackers employed the use of BlackEnergy 3 malware in a phishing attack on three major energy providers within the Ivano-Frankivsk region of Ukraine. When employees downloaded the malicious emails, hackers were able to plant KillDisk malware into the electrical grid causing a six-hour blackout for 225,000 people (SANS 2016: 5-8). 'CRASH OVERRIDE,' an identical cyberattack focused on Kiev, occurred one year later (Greenberg 2017). These incidents marked more than the first use of a cyberattack against a power grid (International Risk Management 2016), as they highlight profound concerns for weaponizing cyberspace.

These events demonstrate the human cost of cyberattacks. Within the Ivano-Frankivsk region and Kiev exist numerous hospitals, power plants, water treatment centers, financial institutions, and government agencies all interconnected and dependent on the same grid. Albeit incurring no deaths, an attack of this nature holds the potential to unravel the fundamental day-to-day operations of a society. Without a functioning hospital, people die.

Without water treatment plants, disease spreads. Financial institutions and industries unable to operate for an extended period of time paralyzes economies. As the consequences mount, a state comes apart at the seams. In addition to these dire straits, the attribution dilemma looms as an ancillary concern. When states cannot perfectly attribute attacks to other states in a pre-existing conflict setting, the creation of a 'grey zone' undermines domestic and international legal systems (Wolitzky, de Mesquita, & Baliga 2019: 12). Thus, a world of growing interconnectivity and rapid technological development without reasonable clarity on global governance mechanisms yields a bleak prediction for the development of modern conflict.

International Humanitarian Law (IHL) and Cyberattacks

In accordance with the mission of the ICRC, IHL serves as a set of rules to limit the effects of armed conflict for humanitarian purposes (ICRC 2004: 2). The principles of IHL are the Martens Clause, the principle of distinction, the principle of proportionality, and the principle of military necessity (ICRC 2019). Regarding the codification of these principles, IHL derives its powers from the four Geneva Conventions of 1949, the Additional Protocols of the Geneva Conventions adopted in 1977 (ICRC 2010), and various treaties banning the development and usage of certain weaponry (Melzer 2011: 5). Regarding cyberattacks, the Fourth Geneva Convention and subsequent Additional Protocols prove most applicable within this domain. Stated in Article 22 of The Hague Convention, 'the right of belligerents to adopt means of injuring the enemy is not unlimited' (ICRC 1907) offers the fundamental idea behind combatting an ever-evolving threat landscape. Albeit central to the conceptualization of *jus in bello*, a clear hindrance lies in Article 36 of the 1977 Additional Protocol stating that, 'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by international law' (UNGA 1977). An assertion meant to address this ever-evolving threat landscape, a lack of widespread understanding around cyberspace undermines the notion from the start. States have entered a digital arena with unclear adversaries, a lack of universal definitions, and a cleavage between engineers and policy makers. The current open-ended working group (OEWG) of the General Assembly sponsored by Russia and Group of Governmental Experts (GGE) sponsored by the United States prove two of these points: the lack of a multistakeholder approach in addressing these gaps in global governance and placing state competition before widespread stability (Grigsby 2018). Given the state of developing cyber norms, present frameworks remain the best springboard for discussing applicability.

In continued attempts to transpose a body of law designed for traditional modes of conflict to a virtual domain, the Tallinn Manual 2.0 presents the sole piece of widely accepted literature addressing the topic. Within Part IV of the Tallinn Manual 2.0, it is established that IHL applies when undertaking a 'cyber operation' within a pre-existing conflict (Schmitt 2017: 68). In the words of the International Court Tribunal for the Former Yugoslavia (ICTY), this is true when the 'operation' is undertaken with a clear 'nexus' between the armed conflict at hand and the operation in question (ICRC 2000). Noting the role of cyberattacks in an international armed conflict and non-international armed conflict, the Tallinn Manual 2.0 affirms the perspective of the ICRC in stating that the legal attributability of a cyberattack is guided by the general international law of state responsibility (Schmitt 2017: 35). The official codification in Rule 14 of Tallinn 2.0 states that, '[A] State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation,' (Schmitt 2017: 59). This view includes a person acting on behalf of a state in a *de jure[15]* or *de facto[16]* capacity (Melzer 2011: 24). Attribution is fundamental to legal responsibility, but attributing a cyberattack proves difficult for the best cyber security experts (SearchSecurity 2019). This fact undermines legal responsibility in its entirety (Rid & Buchanan 2015: 32). When attributing an attack to a state party to a conflict is not possible, IHL bears no explanation on how to proceed; consequently, the lack of clarity around state responsibility destabilizes all underlying principles of IHL in the process.

The law of state necessity, derived from the law of state responsibility, invokes the principle of military necessity. This principle 'permits' the necessary measures needed to achieve a military objective without infringing upon IHL (ICRC 2001). Given the 'downright dangerous' lack of clarity around cyber offensive capabilities (Serbu 2018) and added lack of precedent, applying the concept of 'military necessity' to cyberspace remains in its infancy. Referring to the discussion of attributability, military necessity requires a level of predetermined threat. If a party to a conflict finds themselves at the receiving end of a cyberattack, an inability to 'distinguish' the adversary may lead to an

unpermitted escalation in conflict under IHL, or an act transgressing the principle of proportionality. Thus, the interwoven nature of the principles of IHL allow for an ineffective framework. This dilemma segues into deciding whether or not a cyberattack constitutes an act of 'armed force.' The question itself is twofold, as it raises whether or not a cyberattack can be justified or exacerbate pre-existing conflicts. According to Article 51 of the UN Charter, states hold the right of self-defense in the face of an armed attack (UNGA 1945). Conversely, a cyberattack crosses the threshold of an act of 'armed force' only when the effects are deemed equivocal to an act of kinetic armed force (Serralvo & Dormann 2014: 712). As attribution and lack of precedent remains a pitfall of this argument, interpreting when it is appropriate for a state to repudiate a cyberattack is left to the state's discretion under present norms of conflict. In this case, cyberattacks hold the potential to escalate towards or engage in more severe forms of kinetic conflict evoking grim prospects for technologically advanced conflict (Lin 2012: 51).

The purpose of IHL is to safeguard civilians from the barbarity of war. Under the principle of distinction, parties are required to distinguish between combatants and non-combatants, military objects and civilian objects (ICRC 1977). The concept of combatancy derives from the The Hague Regulations and their consequent adoption of Article 4A within Geneva Convention III (Schmitt 2017: 84). According to Rule 26 of the Tallinn Manual, 'members of the armed forces of a Party to the conflict who, in the course of cyber operations, fail to comply with the requirements of combatant status lose their entitlement to combatant immunity' (Schmitt 2017: 84). As the International Group of Experts for the Tallinn Manual concluded that individual members adopting cyberattacks on civilian infrastructure would fall under the category of unprivileged belligerents, said individuals would be prosecuted under domestic statute (Schmitt 2017: 87). Distinction in cyberspace, as touched on in 2014 by Microsoft's proposed international cybersecurity norms, requires a new range of categories not yet covered by IHL (Microsoft 2014: 4). Aside from understanding one's adversary, undertaking a cyberattack on networks and infrastructure implicates the surrounding populace (Tsagourias & Buchan 2014: 357), as the Internet itself is 90% civilian infrastructure (ICRC 2019: 29). This notion does not imply that all cyberattacks are indiscriminate (ICRC 2019: 36), but the interconnected character of cyberspace challenges the principle of distinction at its core.

The heart of IHL itself exists in the Martens Clause, or the principle of humanity. The Martens Clause states that as treaties and norms develop, citizens and combatants remain under the protection of international law as international law itself is an extension of the 'public conscience' of 'civilized nations' (Peace Palace Library 2019). Given the ongoing developments in analyzing how IHL applies to cyberattacks, scholars and policymakers must remember the human element behind any technology. The ICRC serves as the global vanguard for this principle, and spearheaded a clear analysis centered on the industries most vulnerable to cyberattacks in conflict. The 'human cost' of cyberattacks and key pieces of infrastructure threatened by cyber offensive measures are systems impacting the delivery of essential healthcare, supervisory control and data acquisition (SCADA) industrial control systems, internet services and cloud service providers (ICRC 2019: 10). Regarding medical care, a hospital at full-operability possesses two network systems – those dedicated to administrative data and those embedded in medical devices (ICRC 2019: 18-19). Within a conflict setting, patient information may be exploited to find a specific adversary while an attack centered on medical devices hold the potential to sabotage a needed procedure (ICRC 2019: 19). Noting the threat of cyberattacks against SCADA industrial control systems, this technology regulates valves, motors, and various industrial processes (Goodwin 2018). If targeted within a conflict setting, the system collapse of energy and heavy industry complexes can wreak havoc on the surrounding area (ICRC 2019: 23-24). Moreover, an attack of this nature yields potential for impacting the grid of a city, spurring widespread blackouts mimicking the case in Ukraine. The consequent events drive up the human cost of cyberattacks. Lastly, cloud infrastructure and internet services offers those party to a conflict a high reward target based on interconnectivity (ICRC 2019: 29-30). As previously noted, the internet itself is 90% civilian infrastructure (ICRC 2019: 29), and the legal ramifications prove enormous while invoking the principle of distinction and humanity. Moreover, the symbiotic relationship between IoT and cloud computing allow for real-time analysis and vast data storage for billions of devices. The consequences, on a large scale, cut communication and wireless protocols civilians and military personnel alike depend on (Shea 2019). From cellphones to industry, an attack of this caliber holds the potential to disrupt and dismantle pieces of infrastructure needed to safeguard civilians within an active conflict setting (ICRC 2019: 31). Therefore, in a digital domain wrought with vulnerabilities and mechanisms for attack, assessing the framework of IHL against the use of cyberattacks begs more questions than answers.

Conclusion

The principles of IHL offer the strongest mechanism for protecting civilians amidst kinetic conflict (ICRC 207: 35). Its powers under the Geneva Conventions and Additional Protocols protect all parties to conflict, as conflict itself continues to evolve into a multi-domain endeavor. However, the countless ambiguities in cyberspace, specifically cyberattacks, grant unique challenges to the applicability of IHL (ICRC 2019: 38). It can be deduced that the principles of military necessity, distinction, proportionality, and humanity fall short when addressing the difficulties in attack attribution, lack of precedent and the asymmetric nature of 'cyber conflict' en masse. Given that the majority of cyber operations land below the threshold of kinetic aggression, continued discussion exists as to how international institutions will mitigate combat these 'known threats' (ICRC 2019: 39). Given that these 'known threats' exist in the 'grey zone' between peacetime and conflict, global governance mechanisms in place prove inadequate when addressing the varying scale and present uses of cyberattacks. In spite of this fact, IHL applies to cyberattacks within the context of armed conflict, but to a nominal extent.

The prospect of a conflict occurring solely within cyberspace is far from conceivable at this point in human history (Rees 2018: 85), so international institutions must continue to focus on what is a known security dilemma. Present shortcomings in mitigating the use of cyberattacks demonstrate how technologically advanced states exploit the novelty and lack of regulation around cyber statecraft for political and economic gain. Further, the lack of cooperation between government entities, international institutions and private sector innovation demonstrates a clear vulnerability in developing new norms of state behavior in cyberspace. The imperfections of technology and legal frameworks are due their being an extension of human capability. Humanity can adapt to technological advancement, so global governance frameworks must do the same. If international institutions fail to forge a new digital convention applicable to all contexts and capacities in which cyberattacks occur under the auspices of policy makers and engineers alike, the fabric of humanity's new, interconnected sphere will come apart at the seams.

Bibliography

Aharon, A. (2018). *How Israel is Accelerating Cybersecurity Innovation.* [online]. Available at: https://blogs.timesofisrael.com/how-israel-is-accelerating-cybersecurity-innovation/. [Accessed 17 July 2019].

Buchanan, B. (2019). Artificial Intelligence and Counterterrorism: Possibilities and Limitations. *House Homeland Security Committee,* [online]. Available at: https://homeland.house.gov/imo/media/doc/Testiony-Buchanan.pdf. [Accessed 21 July 2019].

Burt, T. (2019). *New Cyberthreats Require New Ways to Protect Democracy.* [online]. Available at: https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new- ways-to-protect-democracy/. [Accessed 21 July 2019].

Council of Europe. (2001) *Explanatory Report to the Convention on Cybercrime.* European Treaty Series: 4. Budapest, Council of Europe.

Deloitte Perspectives (2019). *Cyber Risk in an Internet of Things World.* Deloitte Corporation. Report number: 4.

The Economist Briefing (2017). *Optical Fibre Made in Orbit Should Be Better than the Terrestrial Sort.* Available at: https://www.economist.com/science-and- technology/2018/09/06/optical-fibre-made-in-orbit-should-be-better-than-the-terrestrial- sort. [Accessed 20 July 2019].

The Economist Briefing (2010). *War in the Fifth Domain.* [online]. Available at: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain. [Accessed 20 July 2019].

ENISA (2018). *Towards Secure Convergence of Cloud and IoT.* [online]. Available at: https://www.enisa.europa.eu/publications/towards-secure-convergence-of-cloud-and-iot. [Accessed 19 July 2019].

FireEye (2019). *Advanced Persistent Threat Groups: Who's Who of Cyber Threat Actors.* [online]. Available at: https://www.fireeye.com/current-threats/apt-groups.html. [Accessed 15 July 2019].

Greenberg, A. (2017). *'CRASHOVERRIDE': The Malware that Took Down a Power Grid.* [online]. Available at: https://www.wired.com/story/crash-override-malware/. [Accessed 19 July 2019].

Goodwin, B. (2018). *Next generation of SCADA industrial controls will protect against cyber attack.* [online]. Available at: https://www.computerweekly.com/news/252439658/Next- generation-of-SCADA-industrial-controls-will-protect-against-cyber-attack. [Accessed 20 July 2019].

Harari, Y. (2019) *The TED Interview: Yuval Noah Harari Reveals Real Dangers Ahead.* [Lecture] TED New York. 17 July.

ICRC (2019). *Fundamental Principles of IHL.* [online]. Available at: https://casebook.icrc.org/glossary/fundamental-principles-ihl. [Accessed 14 July 2019].

ICRC (2017). *Intergovernmental Process on Strengthening Respect for International Humanitarian Law (IHL): Report on Existing Mechanisms, Processes and Initiatives Dealing with IHL.* International Committee of the Red Cross. Report number: 1.

ICRC (2000). *The International Criminal Tribunal for the Former Yugoslavia and the Kosovo Conflict.* [online]. Available at: https://www.icrc.org/en/doc/resources/documents/article/other/57jqd2.htm. [Accessed 21 July 2019]

ICRC (2001). "International Law Commission Report." Resolution A/56/10 of August 10. [online]. Available at: https://casebook.icrc.org/case-study/international-law-commission- articles-state-responsibility. [Accessed 18 July 2019].

ICRC (2019). *The Geneva Conventions of 1949 and their Additional Protocols.* Available at: https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva- conventions/overview-geneva-conventions.htm. [Accessed 19 July 2019].

ICRC (2018). *The Potential Human Cost of Cyber Operations.* International Committee of the Red Cross. Report: 1.

ICRC (2004). *What is International Humanitarian Law?* Advisory Service on International Humanitarian Law. Report: 2.

Institute for Accountability in the Digital Age (2018). *The Hague Global Principles for Accountability in the Digital Age.* [online]. Available at: https://i4ada.org/wp- content/uploads/2018/06/TheHaguePrinciples_public_consultation-v0.1.pdf. [Accessed 21 July 2019].

International Risk Management Institute (2016). *The Growing Threat of Cyber-Attacks on Critical Infrastructure.* [online]. Available at: https://www.irmi.com/articles/expert- commentary/cyber-attack-critical-infrastructure. [Accessed 20 July 2019].

Kessler, S. (2017) Cyberespionage and the Need for Norms. *Harvard Political Review.* [online]. Available at: https://harvardpolitics.com/online/cyberespionage-need-norms/. [Accessed on 18 July 2019].

Knake, R., & Clarke, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* New York, Ecco – HarperCollins.

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Journal of Strategic Studies.* 6(3), 46 – 70. Available at: https://www.jstor.org/stable/26267261?seq=1#metadata_info_tab_contents. [Accessed 19 July 2019].

Lockheed Martin Corporation (2019). *Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense.* [online]. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf. [Accessed 19 July 2019].

McBride, J., & Chatzky, A., (2019). *China's Massive Belt and Road Initiative.* [online] Available at: https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative. [Accessed 9 July 2019].

Melzer, N. (2011). *Cyberwarfare and International Law*. [online] Available at: http://www.unidir.ch/files/publications/pdfs/cyberwarfare-and-international-law- 382.pdf. [Accessed 21 June 2019].

Meron, T. (2000) The Humanization of Humanitarian Law. *The American Journal of International Law.* 94(2), 239-278. Available at: https://www.jstor.org/stable/2555292?seq=2#metadata_info_tab_contents. [Accessed 19 July 2019].

Microsoft (2011). *International Cybersecurity Norms: Reducing Conflict in an Internet- Dependent World.* [online]. Available at: https://www.microsoft.com/en- us/cybersecurity/content-hub/international-cybersecurity-norms-overview. [Accessed 19 July 2019].

Nimfuehr, M. (2018). *Silk Road: A Cautionary Tale about Online Anonymity.* [online]. Available from: https://medium.com/@marcell74/the-silk-road-a-real-thriller-and-the-truth-about- the- anonymity-of-bitcoin-198b519ca397. [Accessed 19 July 2019].

Nye, J. (2019). *Rules of the Cyber Road for America and Russia: Project Syndicate.* [online]. Available at: https://www.belfercenter.org/publication/rules-cyber-road-america-and- russia. [Accessed 18 July 2019].

Panda Security (2019). *Understanding Cyber-Attacks.* [online]. Available at: https://www.pandasecurity.com/rfiles/enterprise/solutions/ad360/1704-WHITEPAPER- CKC-EN.pdf. [Accessed on 17 July 2019].

Peace Palace Library (2013). *The Martens Clause.* [online]. Available at: https://www.peacepalacelibrary.nl/library-special/the-martens-clause/. [Accessed 21 July 2019].

Qadir, A. (2012). *International Law: Recognition, De-Facto and De-Jure Recognition.* [online]. Available at: http://internationallawu.blogspot.com/2012/11/recognition-de-facto-and-de-jure.html. [Accessed on 9 July 2019].

Rid, T., & Buchanan, B. (2014) Attributing Cyber Attacks. *Journal of Strategic Studies.* 38 (1-2), 4-37. Available at: https://www.tandfonline.com/doi/full/10.1080/01402390.2014.977382. [Accessed 18 July 2019].

Rosenbach, E., & Mansted, K. (2019). *The Geopolitics of Information.* [online]. Available at: https://www.belfercenter.org/publication/geopolitics-information. [Accessed 19 July 2019].

Routley, N. (2018). *MAPPED: The World's Networked Undersea Cables*. [online] Available at: https://www.businessinsider.com/map-the-worlds-network-of-undersea-cables- 2017- 8?r=US&IR=T. [Accessed 19 July 2019].

Rubenstein, D. (2014). *National State Cyber Espionage and its Impacts.* [online]. Available a https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf. [Accessed 19 July 2019].

SANS Industrial Control Systems (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case.* [online]. Available at: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf. [Accessed 20 July 2019].

Schmitt, M. ed. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd Edition.

London, Cambridge University Press.

SearchSecurity (2017). *Cyber Attribution.* [online]. Available at: https://searchsecurity.techtarget.com/definition/cyber-attribution. [Accessed 20 July 2019].

Serralvo, J., & Dormann, K. (2015). *Common Article 1 to the Geneva Conventions and the Obligation to Prevent International Humanitarian Law Violations.* [online]. Available at: https://www.icrc.org/en/international-review/article/common-article-1. [Accessed 20 July 2019].

Shea, S. (2019). *Internet of Things (IoT) Devices.* [online]. Available at: https://internetofthingsagenda.techtarget.com/definition/IoT-device. [Accessed 20 July 2019].

Serbu, J. (2018). *Warner: Lack of Clarity on Offensive Cyber 'Downright Dangerous.'* [online]. Available at: https://federalnewsnetwork.com/cybersecurity-2017/2018/12/warner-lack- of-clarity-on-offensive-cyber-downright-dangerous/. [Accessed 22 July 2019].

Tsagourias, N., & Buchan, R. (2014) Is the Principle of Distinction Still Relevant in Cyberwarfare?. *Research Handbook on International Law and Cyberspace.* 1(1), 343 – 365. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2656226. [Accessed 18 July 2019].

US Department of Energy. (2014). *Infographic: Understanding the Grid.* [online]. Available at: https://www.energy.gov/articles/infographic-understanding-grid. [Accessed 21 July 2019].

UNGA (2013). "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." Resolution 66/24 of June 24. [online] Available at: http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf. [Accessed 17 July 2019].

UN (1945). *United Nations Charter.* [online]. Available at: https://www.un.org/en/sections/un- charter/un-charter-full-text/. [Accessed 17 July 2019].

Vavra, S. (2017). *The World's Top Cyber Powers.* [online]. Available at: https://www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276- a2bf- 4a84b4986fe9.html. [Accessed 18 July 2019].

Wallace, D. (2018). *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis.* NATO Cooperative Cyber Defence Centre of Excellence. Paper number: 11.

Wheeler, T. (2018). *In Cyberwar, there are No Rules: Why the World Desperately Needs Digital Geneva Convention.* [online]. Available at: https://foreignpolicy.com/2018/09/12/in- cyberwar-there-are-no-rules-cybersecurity-war-defense/. [Accessed 19 July 2019].

Wolitzsky, A., Sandeep, B., & de Mesquita, E. (2019). *Deterrence with Imperfect Attribution.* Department of Economics, MIT. Report: 1.

World Economic Forum (2019). *Fourth Industrial Revolution.* [online]. Available at: https://www.weforum.org/focus/fourth-industrial-revolution. [Accessed19 July 2019].

World Economic Forum (2019). *Internet of Things (IoT).* [online]. Available at: https://intelligence.weforum.org/topics/a1Gb0000005LWrfEAG?tab=publications. [Accessed 18 July 2019].

Notes

[1] The fundamental change in the way humanity lives, works and relates following extraordinary technological

development (World Economic Forum 2019).

[2] The conditions under which states may resort to war or the use of armed force (ICRC 2019).

[3] The regulations around the conduct of parties engaged in armed conflict (ICRC 2019).

[4] China's proposed infrastructure development and investment initiative that seeks to connect East Asia to Europe vis-à-vis the ancient Silk Road (McBride & Chatzky 2019).

[5] An attack meant to shut down a machine or network, making it inaccessible to its intended users by flooding it with traffic (FireEye 2019).

[6] An attack that relays and possibly alters the communications between two parties who believe they are directly communicating with each other (FireEye 2019).

[7] A social engineering attack used to steal user data (FireEye 2019).

[8] Common method used to spread malware by means of 'drive-by' downloads on insecure websites (FireEye 2019).

[9] Recovering passwords from data stored or transmitted by a computer system (FireEye 2019).

[10] Injecting code that may destroy your database (FireEye 2019).

[11] A type of injection where malicious script is 'injected' into otherwise benign websites (FireEye 2019).

[12] An attack that takes advantage of unsecured network communications to steal data from computers, smartphones and other mobile devices (FireEye 2019).

[13] Cryptographic attack that exploits the math behind the birthday problem in probability theory (FireEye 2019).

[14] Malicious software that takes over a person's computer, make it a botnet, and send malware to other computers (FireEye 2019).

[15] Formal recognition by a government of a requirement under international law (Qadir 2012).

[16] Provisional recognition given by a government if seen to fulfill the requirements of permanence, popular support, and prior international obligations (Qadir 2012).

Written by: Tory Igoe
Written at: Northeastern University
Written for: Professor Denise Garcia
Date written: July 2019