Jus Ad Bellum and Malicious Cyber Operations: A Critical Infrastructure Approach

By

Stephen Lunn

A practicum submitted to the Faculty of Graduate Studies of The University of Manitoba in partial fulfilment of the requirements of the degree of

MASTER OF HUMAN RIGHTS

Faculty of Law
University of Manitoba
Winnipeg

Abstract

The Covid-19 Pandemic has highlighted how important the healthcare sector is as critical infrastructure. It has also revealed how vulnerable the healthcare critical infrastructure is to malicious cyber operations. The number of cyber operations against the healthcare sector has increased substantially since the onset of the pandemic, seemingly unregulated by international law, particularly *jus ad bellum*. This paper argues that cyber operations that target or intend to target healthcare critical infrastructure should be treated as a use of force and armed attack because any intentional disruption to business continuity can and will cause physical harm and potential loss of life. Using the 2017 WannaCry Ransomware attack on the United Kingdom as a case study, this paper analyzes four approaches to classifying a cyber operation as a use of force and armed attack. The first approach is the Instrument Based Approach, which emphasizes a textual reading of the United Nations Charter. The second approach is the Strict Liability Approach, which treats all cyber operations against critical infrastructure as an armed attack. Third, the Effects Based Approach endorsed by the *Tallinn Manual 2.0 on the International Law Applicable to Cyberspace,* which emphasizes the scale and effect of a cyber operation. Fourth, the Cyber Physical System Approach, which emphasizes the intent of the attack.

Finding these approaches insufficient, this paper advocates for a Healthcare Based Approach which would consider any cyber operation rising above the level of espionage on healthcare critical infrastructure as an armed attack.

Acknowledgements

I would like to thank my supervisor, Dr. Bryan Peeler for his constant support and encouragement. Without his kindness and understanding this paper would not have been possible. I would also like to thank Dr. Michelle Gallant for reviewing my paper. Thank you to Mr. and Mrs. Secter, their fellowship has supported my studies and research. Finally, to my Mum and Dad, words will never be enough.

Dedication

I would like to dedicate this paper to my Dad, Kevin Lunn. Your love for learning inspired me to get to the end. We miss you more and more every day.

Table of Contents

List of Tables

Introduction:

In 2017, hospitals and other healthcare facilities in the United Kingdom were affected by the WannaCry Ransomware attack that has since been politically attributed to North Korea by the United States, the United Kingdom, Australia, Canada, New Zealand, Denmark, and Japan.[1] The BBC reported that most of the sector was disrupted by the cyber operation. 6,900 appointments were cancelled by the attack, and overall 19,000 appointments were affected.[2] International response to the attack consisted mainly of political statements and failed to indicate any violation of international law.[3] The international response again fell short with the most significant action taken, being that of the United States, who criminally indicted several North Korean intelligence officers for the attacks.[4] The indictments allow the United States to punish bad actors through their domestic law. It avoided the difficult discussion that States need to have when cyber operations violate international law. The WannaCry attack indiscriminately impacted people, and equally important, harmed the functionality of national healthcare services.

International responses to alleged state-sponsored cyberattacks have generally failed to address core legal issues. States, for a variety of reasons, have both avoided making clear statements in response to an attack and more generally, how International Law applies to cyberspace. The level of contention in this arena has led to general uncertainty, in which states are unclear how to proceed.[5] While States continue to navigate the application of international law, they are joined by academics, Non-Governmental Organizations (NGO's) and international lawyers. Specifically, it is unclear how *jus ad bellum* and the prohibition on use of force enshrined in Article 2(4) of the United Nations (UN) Charter applies. The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual 2.0), which is meant to describe *lex lata* offers the most recent attempt to capture what States think about the application of Article 2(4) to the cyber realm. This issue is particularly important now that attacks such as

[1] Jeremy Wright, "Cyber and International Law in the 21st Century" *Attorney General's Office*" Gov.uk, Attorney General's Office, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[2] Rory Cellan-Jones, "NHS 'could have prevented WannaCry ransomware attack" *BBC.com* 27 October 2017. https://www.bbc.com/news/technology-41753022

[3] Dennis Broeders, Els De Busser and Patryk Pawlak, "Three Tales of Attribution: Criminal Law, International Law and Policy Debates", The Hague Program for Cyber Norms Policy Brief, April 2020, 8.

[4] "North Korean Regime-Backed Programmer Charged With conspiracy to Conduct Multiple Cyber Attacks and Intrusions" justice.gov, Department of Justice, September 6 2018 https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

[5] Eneken Tikk, "International Law In Cyberspace: Mind the Gap" *Cyber Policy Institute* (2020).

WannaCry, and more recently the increasing amount of cyber operations against healthcare during the Covid-19 Pandemic have highlighted the vulnerability of the healthcare sector, and the costs these attacks impose on ordinary civilians.

The literature on the application of the prohibition on use of force identifies three main approaches. First, a strictly textual reading of the United Nations Charter, second a "strict-liability approach, which considers cyber operations on critical infrastructure an armed attack, and third, the effects based approach which consider both scale and effect of the cyber operation. While the jury of States is still very much out on the application of international law and the prohibition on use of force, it is essential that protections are afforded to the healthcare sector across the globe and enforced. For this reason, until States are able to clearly identify and agree on how international law applies to cyberspace, a "healthcare approach" should be adopted and implemented by States. The "healthcare approach" draws upon the "strict liability" approach and the "effects" based approach to offer States a compromise in which attacks on the healthcare sector is banned, while recognizing that certain States may continue to use malicious cyber operations in other sectors. Thus, any malicious cyber operation that targets or intends to target critical infrastructure, such as healthcare, should be treated as a violation of Article 2(4) because any intentional disruption to business continuity can and will cause physical harm and potential loss of life.

This paper will first discuss why cyber operations against healthcare is an important issue that States must pay serious attention to. It will then discuss the relevant approaches to determining if a cyber operation meets the qualification of use of force, and a violation of Article 2(4) of the UN Charter. Following a discussion of the approach and their criticisms, the case studies of Estonia 2007 and WannaCry Ransomware 2017 will be introduced. The approaches will then be applied. There it will demonstrated that no current approach offers satisfactory protection to healthcare critical infrastructure. The argument for a "healthcare approach" will then be presented.

Why healthcare?

The global COVID-19 pandemic has placed enormous pressure on the healthcare sector of every nation. During the pandemic, the number of cyber-attacks against the healthcare sector increased. These attacks affected hospitals, research facilities, supply chains, governments, and international organizations.[6] States have seen a significant increase in malicious cyber operations, in a period where continuity of the healthcare system is absolutely essential to prevent loss of life. For every cyber operation that targets the healthcare system an innocent individual's well-being, health, and life are put at unnecessary risk. From a state and human security perspective these attacks should be seen as unacceptable. Equally as important, people's human rights to life, healthcare and privacy have been violated.

The healthcare sector serves as an almost ideal target for malicious cyber actors because of the need to consistently and constantly access vital data to maintain business continuity and operations. The sector has also seen significant technological advancements in the past twenty years without adequately providing the necessary cyber security measures in certain instances.[7] Many of the systems used are out of date and are vulnerable to malicious codes.[8] Likewise, hospital medical devices are increasingly connected to the hospital Information Communication Technologies (ICT) systems. This allows automatic electronic filing, connecting to biomedical devices, and functioning of medical devices.[9] The increased dependency means that while attacks have increased, the protections have not yet caught up.[10] The International Committee of the Red Cross (ICRC) determined that healthcare infrastructure is vulnerable to malicious cyber operations with serious consequences for health and life should they succeed.[11] Overall, the sector is weak in its cybersecurity leaving it more vulnerable than other areas of critical infrastructure.[12] The interconnectedness of new healthcare technologies to cyberspace creates a serious risk that future malicious cyber operations could be fatal.[13]

[6] "The International Legal and Normative Frameworks to Defend the Health Sector against Cyberattacks" cyberpeaceinstitute.org, CyberPeace Institute, 22 April 2020, https://cyberpeaceinstitute.org/news/2020-04-22-protecting-the-health-sector-the-international-legal-and-normative-frameworks/

[7] "The CyberPeace Institute Launches Cyber 4 Healthcare" cyberpeaceinstitute.org, CyberPeace Institute, 3 June 2020, https://cyberpeaceinstitute.org/news/2020-06-03-the-cyberpeace-institute-launches-cyber4healthcare/

[8] Ibid.

[9] Laurent Gisel, Laukas Zolenjnik, "The Potential Human Cost of Cyber Operations: Executive Summary" *International Committee of the Red Cross,* 14-16 November 2018, 6.

[10] Ibid., 6.

[11] Ibid., 6.

[12] Laurent Gisel, Lukas Zolenjnik, "The Potential Human Cost of Cyber Operations: Full Report" *International Committee of the Red Cross,* 14-16 November 2018, 18.

[13] Ibid., 18.

State and Non-State actors alike are realizing that cyber operations on the healthcare sector are unacceptable. The CyberPeace Institute has argued that “In the midst of the Covid-19, uninterrupted functioning of the health sector and broader healthcare supply chains is essential to prevent a massive loss of life”.[14] This sentiment applies both during the pandemic and outside of it. The continuation of healthcare as essential critical infrastructure means that its continuation is vital. In response to the cyberattacks, the CyberPeace Institute launched the Cyber4Healthcare initiative. They argue that they “cannot accept that healthcare workers fear attacks against their digital infrastructure, attacks that might have physical consequences and threaten human life.”[15]

The ICRC has also been a champion of healthcare and other critical infrastructure at the UN Open Ended Working Group (OEWG). They recommended that “no State should conduct ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.”[16] In International Humanitarian Law, this would be a violation of the Fourth Geneva Convention: Relative to the Protection of Civilian Persons in Time of War of 12 August 1949. Article 18 affords specific protection to hospitals stating “civilian hospitals organized to give care to the wounded and sick, the infirm and maternity cases, may in circumstances be the object of attack, but shall at all times be respected and protected by the Parties to the conflict”[17] Article 20 of the Geneva Convention offers protection to those working in the administration of civilian hospitals.

The ICRC further insist that “States not conduct or knowingly support ICT activity that would harm medical services or medical facilities and should take measures to protect medical services from harm.”[18] At the OEWG, the ICRC voiced their concern regarding the increase of cyber-attacks against the healthcare sector, noting that attacks on healthcare critical infrastructure that disrupts hospital computers, supply chains, and medical devices poses a great risk and danger to those seeking medical services. The ICRC further notes that it is a clear connection to say that if hospitals are not functioning, then lifesaving treatment might not be available.[19] The

[14] “The International Legal and Normative Frameworks to Defend the Health Sector against cyberattacks”

[15] “The CyberPeace Institute Launches Cyber 4 healthcare”

[16] Véronique Christory, “Norms for Responsible State behaviour on Cyber Operations should build on International Law” ICRC.org, *International Committee of the Red Cross,* 11 February 2020.

[17] Article 18 of Geneva IV.

[18] Christory.

[19] “Cyber Attacks against medical facilities pose a real risk to humans – in times of pandemics, in times of conflict, at all times” ICRC.org, *International Committee of the Red Cross,* 2 July 2020,

ICRC called on the members of the OEWG to assert that attacks on healthcare are unlawful and unacceptable.[20]

It is necessary for States to take action through international law to prevent malicious State sponsored cyber attacks against healthcare critical infrastructure. States should adopt "a healthcare first approach" that strictly prohibits targeting a States healthcare critical infrastructure with malicious cyber operations. Under this approach, States would classify all cyber operations against their healthcare critical infrastructure as a use of force as per the United Nations definition of aggression and within the understanding of Article 2(4) of the UN Charter. Healthcare critical infrastructure is vital to the functioning of the State and society. Any cyber operation against the system would simultaneously reach the scale and effect threshold needed to qualify as an armed attack and afford the affected State the right to self-defence, as per Article 51 of the UN Charter.

Literature Review on *Jus ad Bellum* and cyber operations:

Hebert Lin offers the following definition for a cyber-attack. A "cyber-attack refers to the use of deliberate activities to alter, disrupt, deceive, degrade, or destroy computer systems or networks used by an adversary or the information and/or programs resident in or transiting through these systems or networks"[21] This includes attacks such as denial of service and ransomware. Lin claims in this definition that the indirect effects caused by a cyber-attack could be more significant than the immediate effect.[22] This definition encompasses the terms cyber operations and cyber attacks for the purpose of this paper.

There is no universal definition for critical infrastructure. Likeminded States such as the Five Eyes coordinated closely to build common understandings of critical infrastructure and their respective security policies. Australia, Canada, New Zealand, the United Kingdom and the United States agreed to define critical infrastructure as "… as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic

https://www.icrc.org/en/document/cyberattacks-against-medical-facilities-pose-real-risk-humans-times-pandemics-times

[20] Ibid.

[21] Hebert Lin, "Cyber Conflict and International Humanitarian Law" *International Review of the Red Cross* 94, no. 886 (2012), 518-519.

[22] Lin, 518-519.

security, prosperity, and health and safety of their respective nations."[23] Other States, like France for example, define critical infrastructure as "institutions, structures, or facilities that provide the essential goods and services forming the backbone of French society and its way of life".[24] Denmark, in their Cyber and Information Security National Strategy recognized energy, healthcare, transport, finance, telecommunications, maritime, drinking water, and digital services as critical infrastructure.[25] In the case of the Netherlands, critical infrastructure is separated into two categories. Category A includes national transportation, electricity, gas production, oil supplies, nuclear materials, drinking water, and water management.[26] Category B includes regional distribution of electricity and gas, flight management, shipping management, the financial Sector, and government services that depend on digital information and data systems.[27] However, while States may define their critical infrastructure in different ways, or have indicated different areas of critical infrastructure, there are certain common sectors. For example, the Five Eyes all indicate that communications, energy, healthcare and public health, Transportation Systems and Water are areas of critical infrastructure.[28]

No State has ever publicly attributed a malicious cyber operation to another State let alone accused another State of violating the prohibition on use of force in international affairs with such an attack. The prohibition is defined in Article 2(4) of the UN Charter as follows: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[29] The *Tallinn Manual 2.0* and its group of experts

[23] "Critical 5 Forging a Common Understanding for Critical Infrastructure: Shared Narrative" publicsafety.gc.ca, Government *of Canada: Public Safety Canada* March 2014, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/index-en.aspx

[24] "The Critical Infrastructure Protection in France" sgdsn.gouv.fr, *Government of France*, January 2017, http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

[25] "Danish Cyber and Information Security Strategy" ccdcoe.org, *The Danish government: Ministry of Finance*, May 2018, https://ccdcoe.org/uploads/2018/10/Denmark_danish_cyber_and_information_security_strategy_2018_English.pdf

[26] "Official Gazette of the Kingdom of the Netherlands" Overheid.nl, *Government of the Netherlands*, 14 December 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html

[27] "Securing Critical Infrastructures in the Netherlands: Towards a National Testbed" thehaguesecuritydelta.com, *The Hague Security Delta*, 2015, https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf

[28] "Critical 5 Forging a Common Understanding for Critical Infrastructure: Shared Narrative", 2.

[29] UN Charter Art. 2(4)

agreed that a cyber operation such as minor disruption of cyber activities does not always meet the use of force threshold.[30] The same group of experts also noted that there was a lack of consensus on the definitions, criteria, and application of *jus ad bellum* to malicious cyber operations.[31] The *Tallinn Manual 2.0* experts focused on scale and effects of the cyber operation as their definition and approach.[32]

The experts also looked to the 1945 UN drafting conference in San Diego, citing various States rejecting economic coercion as a use of force.[33] They also discussed the considerations of other possible definitions of force including economic and political character.[34] Referencing the International Court of Justice case *Nicaragua v United States*, the experts noted that funding of hacktivists would not be considered force, whereas arming and training hacktivists would meet the use of force threshold.[35] This is not to create analogy between economic coercion and a malicious cyber operation but to emphasize what has historically been included in the definition of force, and what has not.

There is no clear or specific application of the prohibition on the use of force to cyberspace, and certainly not when healthcare critical infrastructure has been targeted. Healthcare critical infrastructure relies on business continuity to maintain lifesaving services and the line between minor disruption and serious consequences at best seems trivial and perhaps may not exist. Two pertinent questions arise in the literature as to when a cyber operation breaches the UN Charter prohibition on the use of force: (i) when does a cyber operation constitute such a violation of the use of force; and (ii) when would a cyber operation constitute an armed attack? The *Tallin Manual 2.0* presents commentary on these questions and attempts to present *lex lata* of the state of international law in this area.

International law makes a distinction between what is considered a use of force and what is considered an armed attack. In international relations, an armed attack is the gravest form of the use of force. The *Tallinn Manual 2.0* makes a distinction between the two, noting that violations of the prohibition on use of force could be responded to by acts of retorsion, countermeasures or

[30] Michael Schmitt. *Tallinn Manual 2.0 On the international law applicable to cyber operations* (Cambridge: Cambridge University Press, 2017), 328, para 1.

[31] Ibid,. 329.

[32] Ibid., 331.

[33] Ibid., 331.

[34] Ibid., 331.

[35] Ibid., 331.

pleas of necessity.[36] In comparison, an armed attack refers to a State's inherent right to self-defence and is covered by Article 51 of the UN Charter. As the gravest form of attack, an armed attack must seriously injure or kill a number of persons or cause significant damage and or destruction of property to satisfy the scale and effect threshold.[37] In response to an armed attack States would legally be able to respond with either a cyber or kinetic response .[38] Given the distinction between an armed attack and use of force, an armed attack needs to reach a certain threshold of severity.[39] In critiquing the conclusions of the *Tallinn Manual 2.0*, Michael Schmitt correctly identifies the question of when does a cyber operation not generating a physical effect rise to the level of an armed attack?[40] Certainly returning to the intent of the attack offers some potential remedy to this question. The "healthcare based approach" fills several gaps in the literature in applying *jus ad bellum* to malicious cyber operations. The healthcare approach focuses on the intent and target of the operation as opposed to the effects produced.

The *Tallinn Manual 2.0* group of experts did consider the viewpoint that multiple cyber-attacks can be aggregated and, if taken together, could meet the scale and effect threshold so as to be considered an armed attack and trigger a State's right to self-defence.[41] Similarly, they addressed the question of whether non-destructive cyber operations can be considered armed attacks. The experts acknowledge the viewpoint where the fallout from a cyber-attack on the stock markets does not directly cause physical damage, it does have a severe impact on civilians and could be considered in the determination if a cyber operation is an armed attack.[42] However, this analysis leaves serious questions unanswered. For example, for self-defence to be considered a legal option, the armed attack must be imminent or ongoing.[43] It could be difficult to assess if an armed attack is on-going should States attempt to argue it is aggregated. As well, the secondary fallout such as a financial market crash due to a cyber operation could also be beyond the ongoing criteria.

[36] Schmitt, "Tallinn Manual 2.0", 337.
[37] Ibid, 341.
[38] Schmitt "Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum", *Harvard National Security Journal* 8, no. 2 (2017): 244.
[39] Ibid., 245.
[40] Ibid., 246.
[41] Schmitt, "Tallinn Manual 2.0", 342.
[42] Ibid., 342.
[43] Schmitt, "Peacetime Cyber Responses"" 246.

Generally speaking, it is understood that the UN Charter applies in full to cyber, including Article 2(4) on the prohibition on use force. This is confirmed in both the 2013 and 2015 UN Group of Governmental Experts consensus reports.[44] While Article 2(4) refers specifically to territorial integrity, political independence, and inconsistency with the purposes of the UN Charter, it is understood that the prohibition applies to "any use of force not otherwise permitted by the terms of the Charter".[45] From this measure, cyber operations against healthcare critical infrastructure could be considered a violation of the prohibition of the use of force. However, controversy exists in how to analyze and frame a "cyber-attack". There are three distinct approaches to classifying cyber operations as a use of force. First there is an instrument based approach which refers to the weapon used. Second is a "strict liability approach" in which all attacks on critical infrastructure are considered use of force. Finally, there is an effects based approach that considers the overall effect of the cyber operation on the victim State.[46]

1. Instrument based approach

The Instrument based approach, which relies on a strict textual reading of Article 2(4), is largely incapable of addressing most cyber operations and would prove to be the most restrictive in addressing attacks specific to healthcare. In part, this is blamed on what Michael Schmitt refers to as a "cognitive shortcut"[47] by focusing on the instruments of coercion used, such as military force.[48] The emphasis is largely on kinetic weapons. Under this approach Nguyen explains that a cyber operation cannot be considered force or an armed attack because the instrument being used, computer code, is not physical or a conventional military force.[49] A cyber operation that destroyed critical infrastructure such as an electrical power grid or disrupted

[44] United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98* (24 June 2013), available from *https://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-0-518.pdf*
United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/70/174 (22 July 2015), available from https://undocs.org/A/70/174

[45] Michael Schmitt, "Cyber Operations and the Jus Ad Bellum revisited" *Villanova Law Review* 56, no. 3 (2011): 571.

[46] Reese Nguyen, "Navigating Jus Ad Bellum in the Age of Cyber Warfare" *California Law Review* 101, no. 4 (2013): 1083.

[47] Robert Jervis. *Perception and Misperception in International Politics.* (Princeton: Princeton University Press, 1976).

[48] Schmitt "Jus Ad Bellum revisited", 573.

[49] Nguyen, 1118.

emergency response communications would not trigger the right to use force in self-defence because it was computer code and not a physical weapon that caused the damage.[50] While it is unlikely that States in practice would readily accept this specific scenario it does demonstrate the broader critique that cyber operations are not well understood by this approach. Prominent scholars such as Schmitt argue that cyber operations that cause physical harm similar to conventional weapons are uses of force. The overall critique that this approach keeps us from addressing new technologies in *jus ad bellum* is valid.

2. Strict Liability Approach

The strict liability approach frames the *jus ad bellum* around the "status of the attack's target".[51] Under this approach, critical infrastructure is given a special status and any cyber-attack against it would be considered an armed attack.[52] Eric Talbot Jensen argues that given the current status of international law on the use of force the right to self-defence should include cyber-attacks on critical national infrastructure, even if the cyber operation itself does not constitute an armed attack in reality.[53] This approach would guarantee that the healthcare sector would be well protected under international law with a zero tolerance policy for malicious cyber operations in place.

Two key criticisms of this approach are that all States define their critical infrastructure in different ways leading to large inconsistencies.[54] Definitions of critical infrastructure could include anything from energy and transportation to commercial facilities. Second, under this approach any cyber intrusion into a critical infrastructure system, such as espionage would qualify use of force and an armed attack.[55] The zero-tolerance threshold is almost entirely unreasonable given State practice in cyber espionage and the legal grey area in which espionage operates. Under this approach Russia, China, and the US would all be at war with each other for committing cyber espionage on critical infrastructure.[56]

[50] Ibid., 1119.

[51] Ibid., 1119.

[52] Ibid., 1119.

[53] Eric Jensen, "Computer Attacks on Critical National Infrastructure: A use of Force Invoking the Right of Self-Defense" *Stanford Journal of International Law* 38, no. 2 (2002): 229.

[54] Nguyen., 1119.

[55] Ibid., 1120.

[56] Ibid., 1120

3. Effects Based Approach

The third approach is the effects based approach. This is the approach taken by the *Tallinn Manual 2.0* which they argue to be *lex lata.* Under this approach cyber-attacks that produce physical destruction similar to a kinetic attack would qualify as use of force or an armed attack.[57] Rule 69 of the *Tallinn Manual 2.0*, which states "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[58] In the commentary on the rule the group of experts agreed that acts that kill or injure persons or physically damage or destroy objects are considered uses of force.[59] By this standard attacks on healthcare that result in the death or injuring of an individual or were to damage or destroy lifesaving medical equipment could qualify as a use of force. This of course would also depend on the scale and effect of the cyber-attack.[60] Michael Schmitt argues that States will consider the severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility when treating a malicious cyber operation as a use of force.[61] The *Tallinn Manual 2.0* notes the same criteria emphasizing the assumption that States will focus on the scope, duration and intensity of the consequences, making severity the most significant factor.[62] The Manual makes this assumption because the approach focuses on the level of harm inflicted. The criteria is used to identify "cyber operations that are analogous to other non-kinetic or kinetic actions that the international community would describe as uses of force."[63]

This effects based approach would exclude operations that do not succeed because they fail to produce an effect or consequence. [64] The varying difference in online capabilities and capacity to shutdown networks also means that a malicious cyber operation on State A might incur different effects than it did on State B.[65] Some consider this framework to be overly broad.[66] Michael Schmitt applied the criteria listed in what would become the *Tallinn Manual*

[57] Ibid., 1122.
[58] Schmitt, "*Tallinn Manual 2.0",* 330.
[59] Ibid., 333.
[60] Ibid., 333.
[61] Schmitt "Cyber Operations and the Jus Ad Bellum Revisited", 577.
[62] Schmitt, "Tallinn Manual 2.0", 334.
[63] Ibid., 333.
[64] Nguyen., 1122.
[65] Ibid., 1124
[66] Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited" 577.

2.0 approach to the 2007 cyber-attack on Estonia. The case used is important given that there were no deaths, injury or physical damage caused by the attack, while causing significant disruption to the entire country.[67] In the case of Estonia, Schmitt argues that the level of severity and immediacy identified in his approach is met because the attack "far exceeded mere inconvenience or irritation. The effects were immediate and, in the case of confidence in government and economic activity, wide-spread and long term."[68] Factors such as directness and invasiveness were also met because the attack made federal funds inaccessible and interfered with core government service delivery, such as government benefits.[69] Directness is arguably met because of the inability to access funds and delivery government services. Invasiveness is met because some of the systems targeted were designed to be secure.[70] Schmitt does recognize that the impact was difficult to quantify given that services were denied as opposed to destruction of data.[71]

While Schmitt concluded that the attack amounted to a use of force[72], using the same criteria Reese Nguyen concluded that the attack did not meet the threshold needed to be considered a use of force.[73] In Nguyen's analysis, it is argued that the effects based criteria are so flexible that different experts studying the same case could determine a violation of use of force where the other finds no violation. Using the same criteria as Schmitt, Nguyen argued that severity was not met given that no one was physically injured, and that the attack only limited access to the Estonia Internet for several hours.[74] The attack was also not immediate because the consequences, such as less trust in the government, were delayed and were not an immediate consequence of the attack.[75] The attack did not meet the threshold of directness because the effects of decreased trust in government were not seen as "direct' compared to the direct loss of access to servers.[76] The threshold of invasiveness was not met because the attack was conducted remotely.[77]

[67] Ibid., 577.
[68] Ibid., 577.
[69] Ibid., 577
[70] Ibid., 577.
[71] Ibid., 577.
[72] Nguyen, 1123-11234.
[73] Ibid., 1123-1124.
[74] Ibid., 1123.
[75] Ibid., 1123.
[76] Ibid., 1123.
[77] Ibid., 1123.

4. Cyber Physical System Approach

Nguyen suggests an approach where cyber-attacks would constitute an armed attack "when they are intended to cause irreversible disruption or physical damage to a cyber-physical system."[78] The cyber physical system approach attempts to address "trivial disruption or damage" as uses of force that do not amount to an armed attack to limit responses to non-forceful means by the victim state.[79] The benefit of this framework is that the target matters. If the intended or actual effect on critical infrastructure would occur and the results could be catastrophic, it would be considered an armed attack. While the inclusion of intent is to be commended, the approach is still problematic. Whereas the strict liability approach and effects based approaches were rightfully critiqued for their over-inclusion and low threshold the cyber physical system approach should be considered as overly restrictive.

WannaCry Ransomware Attack

The WannaCry ransomware attack is one of the most significant and well-known cyber operations that targeted the healthcare sector. The ransomware infected hundreds of thousands of computers across 150 different countries costing millions of dollars in damage.[80] It had incredibly detrimental effects on the United Kingdom healthcare system. Forty-eight National Health Service (NHS) locations were affected by the ransomware, resulting in forced cancellations of appointments and surgeries.[81] Just under seven thousand appointments were cancelled directly because of the attack and the NHS estimated that more than 19,000 appointments were impacted directly or in the aftermath of the attack.[82] One hundred and thirty nine of the appointments cancelled were urgent referrals, including surgeries.[83] The NHS was unable to confirm the impact the attack had on emergency services and information delays.[84] Experts involved in the post-mortem of the attack indicated that the timing of the attack had a

[78] Ibid., 1125.

[79] Ibid.,1125.

[80] Gordon Corera, "Cyber-attack: US and UK blame North Korea for WannaCry" bbc.com, *BBC News,* 19 December 2017, *https://www.bbc.com/news/world-us-canada-42407488*

[81] Ibid.

[82] Cellan-Jones, "NHS 'could have prevented' WannaCry Ransomware attack"

[83] Ibid.

[84] Ibid.

significant impact on the outcome. They noted that if the attack had happened on a Monday in the middle of winter, as opposed to a Friday in Spring, the impact in scheduling, patient volume and cancellations could have been significantly different.[85]

Canada, Australia, New Zealand, Japan, the United Kingdom and the United States all attributed the attack to North Korea based on US intelligence analysis and evidence.[86] The United States attribution of the WannaCry attack failed to indicate if North Korea had violated any specific international obligation. Similarly, the British Foreign Secretary, Lord Ahmad, attributed the attack to North Korea, specifically the Lazarus group, a North Korean based hacking entity, but made no mention of a legal obligation being violated or specifically a member of the North Korean government being involved.[87]

In their attribution statement, the United States indicated that the consequences of the attack were not just economic, citing the impact the ransomware attack had on the United Kingdom's healthcare services, which put lives at risk.[88] The reasons for these omissions speak to the complexity and uncertainty States face in attributing malicious cyber operations. For the purposes of assessing the *jus ad bellum* it is important to select cases where States have made a reasonable indication as to which State they believe was responsible for the original attack.

1. Instrument Based Approach

The instrument based approach offers no protection to the healthcare sector from malicious cyber operations. A purely textual reading of the UN Charter offers no reasonable or concrete method that would find the WannaCry ransomware attack a violation of the Article 2(4) prohibition on the use of force. The standard for finding a violation in this approach is based on how similar the attack was to an attack with conventional weapons.[89] The terms "use of force", "armed attack", and "armed force" are used interchangeably throughout the UN Charter.[90] As these terms are expanded on in different sections of the Charter they offer some indications as to

[85] Ibid.

[86] "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea" *WhiteHouse* 19 December 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

[87] "Foreign Office Minister condemns North Korean actor for WannaCry attacks" *gov.uk, Government of the United Kingdom,* December 19, 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

[88] Ibid.

[89] Nguyen, 1117.

[90] Ibid., 1118.

what is considered "force" and can be referred to in order to provide context.[91] Article 41 and 42 of the Charter details what is and is not considered armed force. Article 41 references the actions available to the Security Council that do not include use of force such as interruption of economic relations, rail, sea, air postal, telegraphic, radio and other means of communications. Article 42 reads "should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstration, blockade, and other operations by air, sea, or land forces of Members of the United Nations".

The context provided by Article 42 suggests that conventional military capabilities such as air, sea and land forces only qualify as uses of force. The differences identified in these two articles suggest that force means traditional military force and excludes the coercive measures identified in Article 41.[92] This is also supported in the UN resolution on the Definition of Aggression in which "aggression" includes armed invasions, port blockades, bombardments and armed violations of territory, and all actions involving physical force and physical territory.[93]

Article 1 of the UN Definition of Aggression defines "aggression" as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations."[94] In reference to use of force, Article 2 notes that the "first use of armed force by a State in contravention of the Charter shall constitute *prima facie* evidence of an act of aggression."[95] Article 3 indicates certain acts that may be considered aggression, such as, a) "invasion or attack by the armed forces of a State of the territory of another state", b) "bombardment by the armed forces of a State against territory of another State or use of any weapons by a State against the territory of another State", c) blockade of ports, d) an attack by the armed forces of a State on the land, sea

[91] Ibid., 1117.

[92] Ibid., 1118.

[93] Ibid., 1118.

[94] General Assembly resolution 3314, *Definition of Aggression,* A/RES/3314(XXIX) (14 December 1974), available from https://undocs.org/en/A/RES/3314(XXIX) pg. 143.

[95] Ibid., 143.

or air forces, of another State. [96] While the criteria are not exhaustive[97], it demonstrates what type of actions were to be considered uses of force.

Using Article 41 and 42 to provide context, the WannaCry ransomware attack would not be considered a use of force. The WannaCry attack infected Windows computers and encrypted files on the hard drive of the targeted computers.[98] It is a computer code that accesses and encrypts data and then locks it until a ransom is paid.[99] WannaCry in no way used air, land, or sea attacks to penetrate and encrypt the UK computer systems to achieve its desired outcome. It is impossible to consider this a use of force using an instrumental/textual approach because a cyber operation is not considered analogous to a conventional weapon. As Nguyen recognizes, this approach does not allow cyber operations to be considered a use of force because the instrument used in a cyber operation is code.[100] This conclusion is consistent with the belief that both the Stuxnet attack on Iran's nuclear centrifuge and the 2007 Estonia distributed denial of service attack are not uses of force under the instrumental approach.[101]

2. Strict-Liability Approach

The strict liability approach affords the United Kingdom the right to self-defence under Article 51 of the UN Charter in response to the WannaCry attack. This approach would recognize that cyber-attacks against a nation's critical infrastructure from any source attributable to a State constitutes a use of force and would trigger a State's right to self-defence under Article 51 of the UN Charter.[102]

The criteria for this approach offer a low threshold for what is considered use of force. This low threshold criterion is based on the assumption that it is unreasonable for a cyber operation that does not cause physical damage or destroy an object to not be considered or amount to a use of force.[103] An act that is initially considered espionage could have results that

[96] Ibid., 143.
[97] Ibid., 143.
[98] Josh Fruhlinger, "What is WannaCry ransomware, how does it infect, and who was responsible?" *CSOonline.com* August 30, 2018. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
[99] Fruhlinger.
[100] Nguyen1118.
[101] Ibid., 1119.
[102] Jensen, 209.
[103] Ibid., 222.

span across a spectrum of impacts depending on numerous factors.[104] Intent is the determining criteria in this approach. If the intruder demonstrates hostile intent, then it should be considered a use of force.[105] Further, Eric Jensen argues that once intent is demonstrated against critical infrastructure, the victim State attains the right to infer malicious intent and take appropriate action in self-defence"[106]

The strict-liability approach would have considered the WannaCry attack on the UK healthcare sector a use of force. The WannaCry ransomware penetrated the UK healthcare sector. Healthcare has been identified as one of their national areas of critical infrastructure.[107] Because healthcare is considered critical infrastructure it would allow the UK to respond in self-defence should they wish. The lower threshold criteria of the attack would have allowed for greater flexibility in responding to the malicious operation should the affected States wished.[108]

However, it is unclear if the specific intent of the WannaCry attack was to target the UK's healthcare system. As indicated, intent and capability are the qualifying factors in this approach. The malicious actor would need to show both malicious intent and the capability to penetrate passive defence and cyber security measures before the target State would be able to claim self defence under Article 51 of the UN Charter. WannaCry impacted 150 different countries and over 300,000 computers across the world.[109] Russian infrastructure was also subject to the attack, with their interior ministry noting one thousand computers compromised, health ministry impacted and domestic banks affected as well.[110] Similarly several Spanish companies responsible for power, and FedEx were also significantly affected.[111] Given the scope and reach of the attack it isn't clear that the intent of the attack was to specifically target the UK's health infrastructure. The ransomware exploited a specific vulnerability in an outdated computer system. It is therefore unclear if the direct intent was to disrupt the functioning of UK healthcare infrastructure or disrupt critical infrastructure in general. The intent may not have

[104] Ibid., 222.
[105] Jensen, 224.
[106] Ibid., 236.
[107] "Critical 5 Forging a Common Understanding for Critical Infrastructure: Shared Narrative", 12.
[108] Jensen, 228.
[109] Corera.
[110] "Massive ransomware infection hits computers in 99 countries" bbc.com, *BBC News,* 13 May 2017, https://www.bbc.com/news/technology-39901382
[111] Ibid.

been to directly target the UK health sector, however the attack did not discriminate in target and was inconsistent with State responsibility in general.

While the strict liability approach would qualify the WannaCry attack as a use of force there are several reservations that must be considered. The strict liability approach treats acts of cyber espionage against critical infrastructure as uses of force, creating a low threshold for the use of force. Any nation that has conducted cyber espionage in the past would then be at war with one another.[112] Cyber operations that rise above pure espionage should be considered a use of force, strictly when targeting the healthcare sector. What is and is not critical infrastructure is a national decision in which each State defines and outlines their critical infrastructure.[113] Normally, this is reflected in national legislation and administrative processes. These designation processes can be both overly inclusive and restrictive depending on the given State.[114] In certain cases, infrastructure can be broken down into categories of most essential to least essential. A key critique is that this approach gives too a low a threshold and depending on how the targeted nation defines critical infrastructure, is too encompassing.[115] It leaves States with too much ability to justify self-defence over cyber operations that penetrates State critical infrastructure.[116]

There are some indicators that States may consider a similar style approach to a strict-liability standard. The government of the Netherlands has indicated that "if there are no actual or potential fatalities, casualties or physical damage" a cyber operation targeting "essential functions of the State could conceivably be qualified as an armed attack… if it could or did lead to serious disruption of the functioning of the State or serious and long-lasting consequences for the stability of the State."[117] Certainly, the WannaCry attack on the UK Healthcare system could be considered in a similar fashion, as it did lead to serious disruption of the functioning of the State. Lord Ahmad stated the WannaCry attack was one of the most significant cyber-attacks to hit the UK terms of scale and disruption.[118]

[112] Nguyen, 1120.
[113] Ibid., 1119.
[114] Ibid., 1119.
[115] Ibid., 1120.
[116] Ibid., 1121.
[117] Schmitt "Peacetime Cyber Responses", 246.
[118] "Foreign Office Minister condemns North Korean actor for WannaCry attacks"

3. Effects Based Approach

The effects based approach adopted by the *Tallinn Manual 2.0* and initially introduced by its Project Lead, Dr. Michael Schmitt is designed to represent *lex lata* in assessing a use of force. The Manual argues that States will likely consider the severity, immediacy, directness, and invasiveness, amongst other criteria.[119] Michael Schmitt applies these considerations to the 2007 cyber-attack on Estonia and concluded that the attack should have been considered a use of force. The WannaCry attack may draw similar conclusions to the ones Schmitt drew in 2011. The Estonia attack caused no deaths, injury or physical damage but did significantly impact the functioning of Estonian society.[120] The criteria used by Michael Schmitt considered the economic damage caused, the impact the attack had on government functions and services, and the impact the attack had on the daily lives of the Estonian people.[121] The consequences of the attack also had to surpass a level of inconvenience and irritation.[122]

In 2007, Estonia was subject to a Russian based cyber operation after a Soviet war memorial was removed from the center of Tallinn.[123] The Government of Estonia was the main target of the cyber operation, with the information systems and infrastructure of the President, Prime Minister, State Audit Office, ministries, political parties, banks, news agencies and Internet services providers all being targets of direct attacks.[124] Estonia, at the time had integrated the internet and digital technology in their society. For example, they relied on digital services for many things under the umbrella of the public service such as banking, filing tax returns, and public transportation.[125] Government employees were unable to communicate with each other via email and the media was unable to deliver news.[126]

The first consideration is severity. The *Tallinn Manual 2.0* states that "consequences involving physical harm to individuals or property will in and of themselves qualify a cyber operation as a use force."[127] This first qualification did not apply to Estonia, as no physical

[119] Schmitt, "Tallinn Manual 2.0", 333-334.
[120] Schmitt "Jus Ad Bellum Revisited", 577.
[121] Ibid., 577.
[122] Ibid., 577.
[123] Ibid., 569.
[124] Ibid., 569.
[125] Ibid., 570.
[126] Damien McGuinness, "How a cyber attack transformed Estonia" bbc.com, BBC News, 27 April 2017, https://www.bbc.com/news/39655415
[127] Schmitt, "Tallinn Manual 2.0", 344.

destruction was caused, nor was there loss of life. Regarding WannaCry and the UK healthcare sector, there were no reported deaths or damage caused. The physical effect and understanding of severity do not apply. The second test found in the severity category is the impact the cyber-attack has on the States critical national interests. The *Tallinn Manual 2.0* further explains that scope, duration, and intensity of the consequences will weigh significantly if States deem the attack severe enough to be considered a use of force.[128] WannaCry did significantly impact one of the UK's critical national interests, healthcare. However, there was no physical damage or destruction. The impact of the attack added significant stress to the healthcare system. Notably, experts have indicated that should the attack have taken place on a different day of the week, the impact of the attack and severity could have been significantly worse.[129]

The standard of immediacy suggests that States will look at how immediate the consequences were. The reasoning is that the longer it takes for the effect to manifest, the more time the impacted State will have to seek alternate accommodations.[130] In the case of Estonia, Schmitt argued that the effects were immediate and long-term.[131] The effects of the WannaCry attack were immediate given that the attack was a ransomware attack, with key information locked by the virus. The immediacy test was reasonably met given that one hundred and thirty-nine urgent surgeries were postponed, 6900 appointments were cancelled, and 19,000 appointments were affected, within days of the virus infecting the respective computer systems.[132]

Directness assesses the link between the attack and the consequence. The *Tallinn Manual 2.0* states that "Cyber operations in which cause and effect are clearly linked are more likely to be characterized as uses of force."[133] There is a direct link between the ransomware and the inability of healthcare professionals to carry out their duties when their computer files are encrypted and rendered in accessible. The invasiveness of the attack is a more complicated factor to consider. It is defined in the *Tallinn Manual 2.0* as "the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State."[134]

[128] Ibid., 344.
[129] Cellan-Jones.
[130] Schmitt, "Tallinn Manual 2.0", 344.
[131] Schmitt, "Jus Ad Bellum Revisited", 577.
[132] Cellan-Jones
[133] Schmitt, "Tallinn Manual 2.0", 334.
[134] Ibid., 349.

Healthcare is considered critical infrastructure in the UK.[135] Medical data and personal information are encrypted, confidential files, a cyber operation that targets these encrypted files should be considered highly invasive. However, intent again matters significantly.

The *Tallinn Manual 2.0* notes that "the more the intended effects of a cyber operation are limited to a particular State, the greater the perceived invasiveness of that operation."[136] In the Estonian case Schmitt argues that the intent was to frustrate the economic functions of Estonian society.[137] The intent of the operation is not as clear in the case of WannaCry. The ransomware had a significant global impact with several other countries and private businesses being adversely affected.[138] While it is reasonable to assume that the actor's intent was to cause significant disruption globally, it is not clear that the specific intended target was the UK's healthcare service, just as it was the Russian intent to disrupt the function of Estonian government.

The criteria provided by the *Tallinn Manual 2.0* and Michael Schmitt are not explicit in how they should be applied to a cyber operation. Schmitt admits that the categories are imprecise. They are quite flexible in how States can apply the criteria and is only considered to be a starting point to guide State practice.[139] The application of these criteria is inconsistent and entirely based on State practice and how they believe international law applies to cyberspace to begin with.

The criteria are so flexible that other authors have applied the criteria to the same case and reached different conclusions.[140] The criteria are not consistent when applied to different States where there are disparities in cyber security capacity. Under this approach, States with stronger cyber capabilities and defence systems could completely mitigate an attack that may be devastating to another State. WannaCry exploited a vulnerability in Windows XP, Microsoft 7 and 10 operating systems respectively. Most infections occurred within the XP and 7 operating systems.[141] By 2017, Windows XP and 7 were also significantly outdated and replaced by the

[135] "Critical 5 Forging a Common Understanding for Critical Infrastructure: Shared Narrative", 12.
[136] Schmitt, "Tallinn manual 2.0", 335.
[137] Schmitt "Jus Ad Bellum Revisited", 577.
[138] "Massive ransomware infection hits computers in 99 countries" BBC News 13 May 2017 https://www.bbc.com/news/technology-39901382
[139] Schmitt "Jus Ad Bellum Revisited", 578.
[140] Nguyen, 1123.
[141] Fruhlinger.

newer operating system, Microsoft 10. More robust and up to date systems were not impacted by the ransomware virus.[142] The technology involved, and the state's ability to procure state-of-the-art software, and inabilities to upgrade cybersecurity measures is an important factor in assessing if a violation of use of force occurred. An effects based approach rules out what the intended consequences of the attack were supposed to be. Unlike a bomb, which States could reasonably agree would have some destructive effect, the same cannot said about cyber operations, unless the attack is successful and the consequences manifest. Because they manifest differently based on a State's capacity, the application of the prohibition would be inconsistent every time an attack was launched.[143]

The armed attack criteria stemming from the effects based approach is unclear if the case of Estonia and WannaCry would meet the scale and effect needed to trigger the right to self-defence. Cyber operations are treated as weapons in the same way that chemical, biological and radiological attacks are considered weapons, and it is recognized that they can cause significant damage, destruction and loss of life.[144] The International Group of Experts in the *Tallin Manual 2.0* agreed that an armed attack meets the scale and effect threshold when a cyber operation "seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement."[145] The criteria for an armed attack appears to be less malleable than that of a use of force. Under the effects based approach, Estonia 2007 and WannaCry would not qualify as an armed attack.

The *Tallinn Manual 2.0* did consider if a cyber operation that did not result in injury, death, damage, or destruction, but caused severe negative effects could qualify as an armed attack but reached no consensus.[146] While some experts maintained that harm and physical damage were the sole deciding factors, others entertained the idea that the effects following the initial destruction or damage could be a deciding factor. [147] Other experts did indicate that a cyber operation against a State's critical infrastructure that causes severe, but not destructive effects could qualify as an armed attack.[148]

[142] Fruhlinger.
[143] Nguyen, 1124.
[144] Schmitt, "Tallinn Manual" 340.
[145] Ibid., 341.
[146] Ibid., 342.
[147] Ibid., 342.
[148] Ibid., 343.

4. Cyber-Physical System Approach.

The Cyber-Physical System approach attempts to address the flaws presented in both the strict liability approach and the effects based approach. Under this approach a cyber operation would need to pose a reasonable risk to international peace and security to be considered a use of force and armed attack.[149] A cyber operation constitutes a use of force and armed attack when it intends to cause "irreversible disruption or physical damage to a cyber-physical system."[150] Acts that endanger life, property and create fear in a population would constitute a violation of the prohibition of use of force but not an armed attack. It is unlikely that WannaCry would be considered an armed attack under this approach. The WannaCry ransomware attack did not target a system that is interconnected with a physical component. An example of an interconnected system would be a computer system that controls an electric grid.[151] WannaCry prevented the access of patient data in the UK and while it caused significant stress to the national healthcare system, it did not cause irreversible damage or injury.

While this approach emphasizes that the intended act is important and recognizes the significance of a particular target, it is overly selective in that only attacks against cyber physical system would trigger the right to self-defence. The rationale is that any State sponsored disruption to a cyber system directly interconnected with the performance of a physical system, such as the performance of an electric grid, or nuclear centrifuge could have the devastating physical effects that *jus ad bellum* seeks to regulate.[152] While Nguyen acknowledges that an attack on cyber systems that has no physical control component could reach the level of armed attack, it would be unlikely to happen.[153] Creating a dual threshold for cyber operations introduces unnecessary barriers to classifying a malicious operation as an armed attack. In an age where society is increasingly connected to cyberspace, it is difficult to predict the impact a malicious cyber operation could have, regardless of whether it targeted a physical system or not. The criterion for this approach essentially requires a direct correlation between the cyber

[149] Nguyen, 1125.
[150] Ibid., 1125.
[151] Ibid., 1126.
[152] Nguyen, 1126.
[153] Ibid., 1125.

operation and a physical outcome, thus drawing similar critiques to the effects based approach introduced by Michael Schmitt.

A Healthcare focused approach

The application of the three approaches to the WannaCry case study demonstrates how difficult it is to classify a cyber operation as a use of force. The strict-liability approach and effects based approach both offer useful considerations that State's should keep in mind when considering the application of international law to the cyber domain. The effects based approach endorsed by the *Tallinn Manual 2.0* is particularly important in guiding State practice in the future. However, the interim must be addressed. State practice has failed to indicate when a violation of international law has occurred let alone a violation of Article 2(4) of the UN Charter. There appears to be a reluctance by States to fully commit to applying the prohibition to the cyber domain in general. States need to balance their interests between regulating cyberspace with international law and still being able to conduct cyber operations themselves. In balancing these interests, cyberspace remains a contentious area where States are unclear how to proceed. The Covid-19 Pandemic and its impact on healthcare has heightened the need for States to indicate how international law applies and hold bad actors accountable.

With that, the healthcare based approach defended here should be adopted immediately by States. This approach would classify all cyber operations above the level of espionage against healthcare critical infrastructure as a use of force as per the UN definition of aggression. This is to build off the normative work done by the ICRC and CyberPeace Institute and reinforce that any cyber attack on healthcare is inconsistent with international law.

The healthcare based approach is meant to act as a middle ground in which States can continue to pursue their interests using cyber operations and continue to deliberate on the application of international law to cyberspace, while healthcare critical infrastructure is protected. The healthcare based approach is grounded in several core principles. Drawing from the strict liability approach, the healthcare based approach adopts the conclusion that a cyber operation against critical infrastructure should be treated as a use of force and armed attack[154], with modifications. Special status would be given to healthcare critical infrastructure alone, with other areas of critical infrastructure not held to the same standard. The healthcare based approach

[154] Nguyen., 1119.

also borrows from the strict liabilities focus on intent. Strict liability concludes that once intent and capability has been demonstrated, the right to self-defence has been granted.[155] The healthcare based approach would use a similar threshold in which once intent and capability has been demonstrated against healthcare critical infrastructure, a State's right to countermeasures and self-defence has been granted.

The principle of intent in the healthcare based approach is to also address the short comings of the effects based approach. In regards to an armed attack, the effects based approach is unclear as to when a cyber operation would meet the required physical damage or injury to be considered grave.[156] It is even further unclear as to when a cyber operation that does not meet such criteria of physical damage or injury can be considered an armed attack.[157] The healthcare based approach would address this gap in international law by considering all cyber operations with malicious intent against healthcare critical infrastructure as an armed attack and use of force. The healthcare based approach also recognizes that an effect would not need to come to fruition. Borrowing from Nguyen's approach, failed cyber operations, that had malicious intent against healthcare critical infrastructure would be considered a use of force an armed attack.

Under the healthcare based approach, the 2017 WannaCry attack would have been considered a use of force an armed attack. The United Kingdom would have had the right to respond with countermeasures or self-defence. In the times of the COVID-19 pandemic, States whose healthcare critical infrastructure have been targets of malicious cyber operations would also have the right to countermeasures and self-defence under the healthcare based approach.

Conclusion

The healthcare based approach is not a permanent solution. It is designed to ensure healthcare critical infrastructure is equally protected across the globe from malicious cyber operations. It is grounded in a desire to protect lives and ensure unobstructed access to vital healthcare services. Its dual purpose is to create a prohibition on the use of cyber operations against healthcare critical infrastructure while States continue to deliberate how international law applies to cyberspace, and how to apply the prohibition on use of force and the right to self-

[155] Jensen, 237.

[156] Schmitt, "Peacetime Cyber Responses", 246.

[157] Ibid., 246.

defence. The value of this approach is its desire to balance basic human needs and right to healthcare while recognizing that States have certain interests in cyber operations.

The healthcare based approach is challenged by two issues which are not easily resolved. First, legal attribution will continue to be a challenge for States regardless of which approach a State chooses to employ. Secondly, the healthcare approach's low threshold could be seen as advocating for conflict. The aim is to create a bright red line of deterrence in which malicious actors are aware of the high price that would be imposed on them should they choose to cross it. The aim is not to cause conflict, but to be clear to States, and non-State actors attributable to a State, how international law applies, and that attacks on healthcare will not be tolerated.

This approach is a band-aid on the larger problem of how international law applies to cyberspace. With the final draft statement of the UN OEWG released on 11 March 2021 and future deliberations ahead, the discussion remains very much in its infancy. Given the various approaches outlined in this paper, States, academics, and Non-Governmental Organizations should continue to consider the effects based approach advocated for in the *Tallinn Manual 2.0*. The findings of the *Tallinn Manual 2.0* should continue to inform States on how to apply international law to cyberspace over the long term.

Bibliography

Broeders, D. Busser, E.D Pawlak, P. "Three Tales of Attribution in Cyberspace: Criminal Law, International Law, and Policy Debates" *The Hague Program for Cyber Norms Policy Brief* (2020)

Christory, V. "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law" icrc.org, *International Committee of the Red Cross* 11 February 2020. https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law

Cellan-Jones, "NHS 'could have prevented' WannaCry Ransomware Attack" *bbc.com, BBC News,* 27 October 2017. https://www.bbc.com/news/technology-41753022

Corera, G. "Cyber-attack: US and UK blame North Korea for WannaCry" bbc.com *BBC News* 19 December 2017. https://www.bbc.com/news/world-us-canada-42407488

"Critical 5 Forging a Common Understanding for Critical Infrastructure: Shared Narrative" publicsafety.gc.ca, *Government of Canada: Public Safety Canada* March 2014. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr/2016-frgng-cmmn-ndrstndng-crtcalnfrstrctr-en.pdf

"Cyber attacks against medical facilities pose a real risk to humans – in times of pandemics, in times of conflict, at all times" ICRC.org, *International Committee of the Red Cross*, 02 July 2020. https://www.icrc.org/en/document/cyberattacks-against-medical-facilities-pose-real-risk-humans-times-pandemics-times

"Danish Cyber and Information Security Strategy" ccdcoe.org, *The Danish Government: Ministry of Finance*, May 2018. https://ccdcoe.org/uploads/2018/10/Denmark_danish_cyber_and_information_security_strategy_2018_English.pdf

"Ensuring Cybersecurity for Critical Civilian Infrastructure" *CyberPeace Institute*, 9 June 2020, https://cyberpeaceinstitute.org/blog/2020-06-11-ensuring-cybersecurity-for-critical-civilian-infrastructure

"Foreign Office Minister condemns North Korean actor for WannaCry attacks" *Gov. UK* 19 December 2017 https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

Fruhlinger, “What is WannaCry ransomware, how does it infect, and who was responsible? *CSOonline.com.* https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

General Assembly resolution 3314(XXIX), *Definition of Aggression*, A/RES/3314(XXIX) (14 December 1974), available from https://undocs.org/en/A/RES/3314(XXIX)

Gisel, L. Zolenjnik, L. “The Potential Human Cost of Cyber Operations: Executive Summary” *International Committee of the Red Cross* 14-16 November 2020.

Gisel, L Zolenjnik, L. “The Potential Human Cost of Cyber Operations: Full Report” *International Committee of the Red Cross* 14-16 November 2018.

Jensen, E. “Computer Attacks on Critical National Infrastructure: A use of Force Invoking the Right of Self-Defense” *Stanford Journal of International Law*, 28(2) (2002): 207-240.

Jervis, R. *Perception and Misperception in International Politics*. Princeton: Princeton University Press, 1976.

Lin, H. “Cyber Conflict and International Humanitarian Law” *International Review of the Red Cross* 94, no. 886 (2012): 515-531.

“Massive ransomware infection hits computers in 99 countries” *BBC News* 13 May 2017. https://www.bbc.com/news/technology-39901382

McGuinness, D. “How a cyber attack transformed Estonia” bbc.com, *BBC News*, 27 April 2017. https://www.bbc.com/news/39655415

Nguyen, R. “Navigating Jus Ad Bellum in the Age of Cyber Warfare” *California Law Review* 101, no. 4 (2013): 1079-1130.

“North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions” justice.gov, Department of Justice, 6 September 2018. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

“Official Gazette of the Kingdom of the Netherlands” Overheid.nl, *Government of the Netherlands*, 14 December 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html

“On the Application of International Law in Cyberspace” auswaertiges-amt.de, *The Federal Government of Germany,* March 2021. http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

"Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea" *Whitehouse* 19 December 2017 https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

"Securing Critical Infrastructures in the Netherlands: Towards a National Testbed" thehaguesecuritydelta.com, *The Hague Security Delta*, 2015. https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf

Schmitt, M. "Cyber Operations and the Jus Ad Bellum Revisited" *Villanova Law Review*, 56 no 3. (2011): 569-606.

Schmitt, M. "Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An analytical vade mecum" *Harvard National Security Journal* 8, no. 2 (2017): 239-282.

Schmitt, M. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Tikk, E. "International Law in Cyberspace: Mind the gap" *Cyber Policy Institute* (2020)

"The Critical Infrastructure Protection in France" sgdsn.gouv.fr, *Government of France*, January 2017. http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf

"The CyberPeace Institute Launches Cyber 4 Healthcare" *CyberPeace Institute* 3 June 2020

"The International Legal and Normative Frameworks to Defend the Health Sector against cyberattacks" cyberpeaceinstitute.org, *CyberPeace Institute* 20April 2020. https://cyberpeaceinstitute.org/news/2020-04-22-protecting-the-health-sector-the-international-legal-and-normative-frameworks/

United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* A/68/98 (24 June 2013), available from *https://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-0-518.pdf*

United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security:*

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the context of International Security, A/70/174 (22 July 2015), available from https://undocs.org/A/70/174

Wright, J. "Cyber and International Law in the 21st Century" gov.uk, Attorney General's Office, 23 May 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Annex 1. *Jus Ad Bellum* Approaches to Cyber Operations

	Is it considered a weapon?	**Criteria**	**Attack on Healthcare considered an armed attack?**
Instrument Based Approach	The strictly textual reading of Article 2(4) of the UN Charter does not allow for a cyber operation to be considered a weapon.	The instrument of attack must be a physical weapon which produces a kinetic effect.	A cyber-attack on critical infrastructure would not trigger the right to self-defence or be considered a use of force.
Strict-liability Approach	Emphasis is placed on the target instead of the means of attack. A cyber operation would be considered a weapon.	The cyber operation must demonstrate intent and capability to penetrate a secure system of critical infrastructure. Any cyber operation against critical infrastructure is an armed attack.	A cyber-attack on critical infrastructure would trigger the right to self-defence and be considered a use of force.
Effects Based Approach	Emphasis is placed on the effects produced. A cyber operation would be considered a weapon.	A cyber operation is considered a use of force or armed attack when it produces an effect similar to physical destruction or kinetic force.	A cyber-attack on critical infrastructure would trigger the right to self-defence if the scale and effect threshold hold was met and the effect was similar to that of a kinetic attack.
Cyber-Physical Systems Approach	Emphasis is placed on the intent of the perpetrator. A cyber operation would be considered a weapon.	Must cause or intend to cause irreversible damage or disruption to a cyber physical system.	A cyber-attack on critical infrastructure would trigger the right to self-defence when the attack is intended to cause irreversible damage or disruption to a cyber physical system.