THE ISSUE OF IMMINENCE: CAN THE THREAT OF A CYBER-ATTACK INVOKE THE RIGHT TO ANTICIPATORY SELF-DEFENCE UNDER INTERNATIONAL LAW?

Samantha Ria Shahriar[*]

Abstract: As States increasingly rely on cyber technology, the threat of international cyber-attacks perpetrated by States and non-State actors continues to grow. To lawfully use force in anticipation of a cyber-attack, it is crucial that the potential attack qualifies as an 'armed attack' under Article 51 of the UN Charter. The prospective cyber-attack also needs to be 'imminent'. Despite there being consensus over some cyber-attacks rising to the level of an 'armed attack', it is nonetheless unclear — both theoretically and practically — whether cyber-attacks can be 'imminent'. This article applies two approaches of 'imminence' to the context of cyber warfare to determine whether anticipatory self-defence can be invoked in these instances. Indeed, as detection capabilities amongst technologically advanced States continues to develop, it is more likely for cyber-attacks which qualify as 'armed attacks' to be detected far in advance. Thus, in providing this theoretical analysis of 'imminence', it will be established whether, in practice, the 'last possible window' in which to stop a prospective cyber-attack has already passed, or is likely to close. This article submits that due to a myriad of complex reasons, it remains unviable for States to invoke the right to anticipatory self-defence in response to a prospective cyber-attack.

A. INTRODUCTION

Cyber technology has been increasingly used by States as a means of running their country efficiently, therefore, attacks focussed on impairing a State's cyber network may be considered an essential offensive tool by enemy States or non-State actors.[1] With the threatening prospect of international cyber warfare becoming progressively more likely, and various forms of cyber-attacks having taken place in recent times,[2] the notion of such attacks has become well founded amongst States, with many developing various preventive and responsive methods to counter

[*] First class LL.B. (Hons) in Scots and English Law (University of Aberdeen), LL.M. in International Law (UCL). I would like to express my gratitude towards Professor Zeray Yihdego and Dr Irene Couzigou (Aberdeen) for supervising an earlier version of this article and Dr Ralph Wilde (UCL) and the editorial team of the UCL Journal of Law and Jurisprudence for their helpful comments. I would also like to thank my family and friends for their continued support. All errors and omissions are my own.

[1] 'Non-State actor' refers to terrorist, rebel or other organised groups and/or individuals located in a foreign territory.

[2] Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited' (2011-2012) 56 Villanova Law Review 569, 569-571.

them.[3] Perhaps the most common and well known cases involving cyber-attacks against a State include the large-scale cyber operations against Estonia in 2007,[4] the Stuxnet cyber-attack on Iran's nuclear program in 2010,[5] and the 2017 cyber-attack on the United Kingdom's National Health Service.[6]

Usually, cyber-attacks tend to impact networks or individual computers, however, such attacks can also affect externally connected systems, facilities or people. Therefore, the destruction or manipulation of a State's cyber network may hold the primary aim of harming tangible, physical targets. Hence, for the purposes of this article, a 'cyber-attack' will refer to instances involving international cyber operations, where deliberate actions are taken against a State's interests aiming to 'disrupt, deceive, degrade, manipulate or destroy information resident in the target information system or computer networks of the systems or networks themselves'.[7]

A great deal of discussion has been devoted to the rising prevalence of cyber-attacks, considering the approaches States can lawfully adopt in these situations. Under Article 51 of the United Nations Charter, contemporary public (customary)[8] international law provides the right to self-defence. Here, it expresses that '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations…',[9] thus offering an exception to the general prohibition on the use

---

[3] National Security Council, 'The Comprehensive National Cybersecurity Initiative' (2009) <https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative> accessed 4 May 2020; The UK Cyber Security Strategy Protecting and promoting the UK in a digital world (Cabinet Office 2011) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> accessed 4 May 2020.

[4] Damien Mcguinness, 'How a cyber attack transformed Estonia' *BBC News* (27 April 2017) <https://www.bbc.co.uk/news/39655415> accessed 4 May 2020.

[5] Josh Halliday, 'Stuxnet worm is aimed to sabotage Iran's nuclear ambition, new research shows' *The Guardian* (16 Nov 2010) <https://www.theguardian.com/technology/2010/nov/16/stuxnet-worm-iran-nuclear> accessed 23 February 2019.

[6] Comptroller and Auditor General, Department of Health, 'Investigation: WannaCry cyber attack and the NHS' *National Audit Office* (25 April 2018) <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf> accessed 23 February 2019.

[7] Joint Chiefs of Staff, Joint Pub 3–13, Joint Doctrine for Information Operations GL-5 (9 October 1998) <https://www.hsdl.org/?view&did=3759> accessed 28 February 2019.

[8] *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)* (Merits) [1986] ICJ Rep 14 para 176.

[9] Charter of the United Nations (adopted 24 October 1945) 1 UNTS XVI, hereinafter referred to as the 'the Charter'.

of force found under Article 2(4) of the Charter.[10] Although a clear standard as to what constitutes an 'armed attack' under Article 51 does not exist, it is generally accepted that the use of force is characterised by the gravity of its effect, as opposed to the particular instrument used.[11] It is also accepted by commentators that some cyber-attacks could rise to the level of an 'armed attack', thus invoking the right to self-defence, provided that other conditions are also met.[12]

More contentious however, is whether the right to self-defence can be triggered, not in response, but rather in anticipation of a cyber (armed) attack. This begs the question of whether the threat of a cyber-attack can invoke the right to anticipatory self-defence. Anticipatory self-defence itself remains a controversial aspect of international law, with some academics questioning its overall validity.[13] However, as the threat of cyber-attacks continues to grow, it is evident that this area of law needs to be clarified and addressed. This is particularly crucial due to the expeditious nature of these attacks, as once they are launched, it is often too late for a State to effectively defend itself from the potentially unimaginable harms. Furthermore, as detection capabilities amongst technologically advanced States continue to rise,[14] it would seem illogical and detrimental for States not to be able to take preventative measures once they are aware of an impending cyber-attack, instead, having to suspend any action until after it has materialised.

In order to determine whether anticipatory self-defence can be relied upon in response to the threat of a cyber-attack, Section B of this article analyses the circumstances under which a cyber-attack can tantamount to the use of force prohibited under Article 2(4). Section C assesses the instances where cyber force can potentially constitute an 'armed attack' under Article 51, whilst also discussing the issue of authorship within the context of cyber warfare. Upon establishing whether some cyber-attacks can invoke the right to self-defence, Section D focuses on the legitimacy of anticipatory self-defence within international law, considering it in line with Article 51 and the *Caroline* doctrine. Here, commentary is also made on pre-emptive and preventive self-defence, which is often argued as being an expansion to the doctrine of anticipatory self-defence. Section E will critically analyse the element of 'imminence' found under

---

[10] ibid (including Article 42, which empowers the United Nations Security Council to authorise the use of force when necessary).

[11] *Nicaragua v USA* (n 8) para. 39.

[12] A State must be able to demonstrate that it is a victim of an 'armed attack' as per *Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America)* [2003] ICJ Rep 161. Furthermore, States must act in accordance with the laws and principles of international law, as will be discussed in this article.

[13] Christine Gray, *International Law and the Use of Force* (4 edn, OUP 2018) 170-175.

[14] Ryan Hayward, 'Evaluating the "Imminence" of a Cyber Attack for the Purposes of Anticipatory Self-Defence' (2017) 117 Columbia Law Review 399, 418. This aspect will be explored in further detail in Section E.

anticipatory self-defence, applying two different interpretations of it to a cyber context. This will help to ascertain which approach is most suitable for States to legally invoke anticipatory self-defence, in response to a cyber-attack. Finally, Section F will shed light on whether the theoretical interpretation of 'imminence' decided upon in Section E can be applied to the operational reality of cyber-attacks in instances where they are conducted on their own, or in conjunction with kinetic weaponry. This article will conclude that although in theory a State can invoke anticipatory self-defence in response to the threat of a cyber-attack, the practical reality remains that for several reasons, it is unlikely that States will be legally able to do so.

B. CYBER-ATTACKS AS A USE OF FORCE

Article 2(4) of the Charter acts as the cornerstone of international law, where it provides that States '…shall refrain in their international relations from the threat of use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposed of the United Nations'.[15] When observing this article in conjunction with the entire Charter, it can be ascertained that 'force' refers to armed military force, with its scope extending neither politically nor economically. This interpretation is evidenced with the consistent mention of 'armed force', in Article 41, 46 and paragraph 7 of the Preamble of the Charter.[16] This is further confirmed by the preparatory work of the Charter, which stipulates that it is concerned with armed military force[17] and State practice.[18]

In establishing this, it must be examined what constitutes as 'armed force' to ascertain whether a cyber-attack can potentially reach the threshold of an 'armed attack' for the purposes of self-defence under Article 51. When observing the Charter and the case-law of the International Court of Justice (ICJ), it is evident that both have failed to clearly define 'armed force'. Usually, the term 'armed' refers to an entity who is either equipped with, or involving the use of, a weapon.[19] Ordinarily, a 'weapon' refers to an instrument which is 'designed or used for inflicting bodily harm or physical damage'.[20] Although the Charter (as supported by the ICJ), fails to provide a list detailing specific weapons in relation to armed force under Article 2(4),

---

15 Charter of the United Nations (n 9).

16 ibid.

17 *Documents of the United Nations Conference on International Organisation*, 1945, Vol. VI, 559 and 720.

18 Irene Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (ESIL 10th Anniversary Conference, Conference Paper No.16/2014 6, Vienna, 4-6 September 2014) <https://ssrn.com/abstract=2593868> accessed 16 February 2019.

19 Bryan Gardner (ed), *Black's Law Dictionary* (8th edn, St Paul Minn, Thomson West 2009) 115, 1730.

20 *Oxford Dictionary of English* (2nd ed, OUP 2008) 1994.

it does however focus its attention more so on the extent of the force employed.[21] Therefore, it can be held that cyber technology could possibly be considered a 'weapon', providing it is used to damage or destroy persons or property.

As iterated by many scholars, offensive action relying upon cyber technology can exemplify 'armed force' depending on the type of approach followed. These approaches can be theoretically utilised as a means of mitigating the discrepancy between cyber technology and the laws on armed conflict, especially as the framework existent under the Charter is particularly outdated in the context of cyber warfare.[22] Although many approaches exist, the primary ones which will be considered are the instrument, consequence and target-based approaches.

1. Instrument-Based Approach

The methodology applied here centres around the traditional investigation of whether a specific act can constitute an example of 'armed force' and thus have the potential of reaching the threshold of an armed attack. Therefore, the point of interest is around the particular instrument used in asserting force - that being kinetic, military force.[23] Hence, in using this approach, a cyber-attack can only be considered an armed attack if it employs conventional military weapons. In following this approach, cyber-attacks will automatically fail to suffice as 'armed force' as they do not possess characteristics which are ordinarily attributed to kinetic, military force.[24] By extension, it will be unable to rise to the level of an 'armed attack'. This is reiterated by the fact that physical force is understood as having an 'explosive effect with shock waves and heat',[25] characteristics which cyber technology does not inherently possess.

Nevertheless, some academics approve of adopting the instrument-based approach on the basis of legal reasoning. For example, Article 41 of the Charter explicitly mentions certain measures the Security Council can take which do not involve the use of armed force, such as: '(…) the complete or aerial interruption of….telegraphic, radio, and other means of communication (…)'.[26] The article implicitly bolsters the logic of the instrument-based approach, where cyber technology, like the aforementioned measures in the article, would too fall short in being

[21] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, para 39.
[22] Irene Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (n 18) 6-8.
[23] ibid 6.
[24] Duncan Hollis, 'Why States Need an International Law for Information Operations', (2007) 11 Lewis & Clark Law Review 1023, 1041.
[25] Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press 1963) 362.
[26] Charter of the United Nations (n 9).

categorised as a use of armed force in international law.[27] In adopting this standpoint, it appears from the outset that other forms of aggression may be better suited to fulfilling the requirements of what constitutes an 'armed attack' under the Charter.

Irrespective of this, the simplistic nature of the approach completely fails to take into account instances where cyber technology has been used as an offensive tool against States.[28] This is because it relies solely upon the use of force in having kinetic characteristics. Therefore, it would be inappropriate to apply this approach to the context of cyber warfare and use it as a model in determining which instruments constitute a form of armed force.

2. Consequence-Based Approach

In contrast to the above-mentioned, the consequence-based approach adopts a more flexible framework, where instead of paying attention to the specific type of weapon used, it focuses on whether the overall effects of an attack are equivalent to those of a traditional military weapon.[29] Therefore, this approach is likely to be adaptable by allowing the possible inclusion of cyber-attacks to qualify as a form of 'armed force', and by extension, potentially reach the requisite level of an 'armed attack' for the purposes of self-defence.[30] It also helps to bridge the gap between what was historically relevant during the drafting of the Charter in 1945, and the current position of contemporary warfare, where technological evolution has arguably contributed to the creation of more sinister and unprecedented threats to international peace and security.

The instrument-based approach has often been adopted by leading scholars when considering the use of chemical and biological agents which have the primary purpose of directly destroying tangible property and/or life.[31] In using such agents for destruction, they ultimately bear resemblance to traditional weapons which involve the use of armed force. A similar line of reasoning can be adopted under the consequence-based approach, where some cyber operations can be used to damage or destroy property or persons in a manner likewise to traditional weapons, thus rising to the level of armed force. Examples of this can be seen, inter alia, when cyber force is used to disable air traffic control systems causing airline crashes,[32] to shut down or disrupt the power or software in hospitals, or cyber operations which control or disable oil

[27] Hollis (n 24) 1041
[28] Mcguinness (n 4); Halliday (n 5); and Comptroller and Auditor General, Department of Health (n 6).
[29] Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (n 18) 6-8.
[30] ibid.
[31] Brownlie (n 25) 362.
[32] Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (n 18) 3, 7.

refineries and nuclear power plants, releasing harmful effluents or radioactive materials. Such uses of cyber technology can ultimately lead to harmful consequences, causing destruction or damage to material property or life. Thus, the severity of such attacks can tantamount to 'armed force' which uses kinetic weaponry.

If carried out with the intention of causing material harm and destruction,[33] similar to those caused by kinetic military weaponry, the consequence-based approach appears to be the most appropriate model in allowing some cyber-attacks to rightfully constitute a form of armed force. Adherence to this approach is also highlighted by State practice and views, where not only do States opine that cyber technology has brought forth a new form of warfare, but have also themselves, invested in advanced forms of cyber capabilities, introducing them into their military operations.[34]

3. Target-Based Approach

The target-based approach is an additional method which has been developed by some commentators to help categorise cyber-attacks which target a State's critical infrastructure as being a form of armed force.[35] Such attacks are viewed as an example of armed force due to the potential severity of the outcome they could cause if an infrastructure were to be impaired.[36] Although no clear definition exists regarding what 'critical infrastructure' constitutes, it is generally accepted by States that they include services such as, health, energy, and water distribution, amongst others.[37] This approach is accepted by States such as the US, who hold that even in the absence of physical injury or damage, the potential damage a cyber-attack could cause to a State's essential functions, would, in the long-term, create severe incapacities which are unlikely to be remedied within a reasonable period of time.[38]

Irrespective of this, cyber-attacks against a State's critical infrastructure lack the necessary immediacy required to determine the final outcome of the attack, thus limiting any assessment on the severity of such an attack. They may not necessarily cause immediate damage or destruction to material objects or persons. Instead, it is more likely that they would only

---

[33] *Islamic Republic of Iran v United States of America* (n 12), para 64; An 'armed attack' must be carried out with the specific intent to harm.

[34] New York Times, 'A New Kind of Warfare' (9 September 2012) <http://www.nytimes.com/2012/09/10/opinion/a-new-kind-of-warfare.html> accessed 18 February 2019.

[35] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 Journal of Conflict & Security Law 229, 231-232.

[36] Reese Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 California Law Review 1079, 1120.

[37] Sean Condron, 'Getting It Right: Protecting American Critical Infrastructure in Cyberspace' (2007) 20 Harvard Journal of Law and Technology 403, 415-416.

[38] ibid 406-408

create a substantial amount of disruption, with the possibility of the lives of individuals within the State's territory, being irritated.[39] Hence, such attacks would only cause certain 'critical' services to be rendered unavailable, rather than damaging or destroying material objects or persons, therefore limiting its ability to be characterised as a form of 'armed force'. Additionally, the uncertainty around the definition of 'critical infrastructure' (where it is not precisely defined by treaty law), can facilitate States to arbitrarily determine which services are to be considered 'critical' in order to invoke the right to self-defence. Furthermore, by invoking the right to self-defence (and indeed, anticipatory self-defence) on the mere assumption that a cyber-attack has been conducted with the malice intent[40] of impairing a State's critical infrastructure - despite having no knowledge of the final level of damage caused - this approach is seen to also be in clear contradiction with the customary principle of 'necessity and proportionality'.[41]

Moreover, in considering the target-based approach to ascertain whether a cyber-attack can qualify as a use of force (and therefore amount to an armed attack), the traditional understanding of what constitutes an 'armed attack' is departed from. As supported by the ICJ, an 'armed attack' is illustrated as being a 'grave use of force', which arguably, any attack to a State's critical infrastructure cannot be.[42] Wide rejection of this approach is also highlighted through State practice, where the attacks suffered by Georgia against its critical infrastructure in 2008, failed to qualify as an armed attack.[43] Similarly, the recent cyber espionage by Russia in 2016 to disrupt the American electoral process is also argued by many academics as not being an act of aggression, despite causing possible harm to the representative democracy of the country.[44]

In sum, the advent of cyber-attacks within modern warfare has often made it challenging to establish the nefariousness of such attacks. Nevertheless, as agreed by many scholars, the international community is more likely to look at the consequences of an attack as opposed

---

[39] Michael Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum' (2017) 8 Harvard National Security Journal 239, 267.
[40] *Islamic Republic of Iran v United States of America* (n 33) para 64.
[41] *The Caroline case,* 29 *Brit. & For St. Papers* 1137 (1841); Use of force by a State in self-defence must be necessary ('instant, overwhelming and leaving no choice of means, and no means for deliberation'), with the response being proportionate to the threat encountered.
[42] *Nicaragua v USA* (n 8) para. 145; Section C will discuss the requirements of an 'armed attack' (in relation to 'armed force'), further.
[43] Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence 2010) 14-33.
[44] Hayward (n 14) 410.

to its nature. Thus, as shown, States can rely on the consequence-based approach in evaluating whether some cyber-attacks may constitute 'armed force', providing that the impact it could cause is of similar equivalence to traditional kinetic weaponry which can create material damage or destruction to tangible objects and persons. Therefore, under this approach, some cyber-attacks can possibly qualify as a form of 'armed force', and by extension, could potentially be demonstrative of an 'armed attack', ergo enabling the international law on self-defence to be applicable in this area.[45]

C. CYBER-ATTACKS QUALIFYING AS AN ARMED ATTACK

As explored previously, certain uses of cyber technology may qualify as a use of force. However, it must be determined whether these offensive cyber operations cross the threshold of an 'armed attack' set by Article 51, as it is not necessary that every instance of armed force qualifies as such. This restriction is illustrative of another way in which the Charter places a limit on the unilateral recourse to the use of force, thus staying in accordance with the intentions of international law to preserve international peace and security.[46]

1. Cyber-Attacks as a Grave Use of Force

In ascertaining whether a use of armed force constitutes an armed attack, the scope, duration and intensity of the force must be assessed.[47] The 'Definition of Aggression' in Article 3(g) of the 1974 UN General Assembly Resolution can be relied upon in establishing what constitutes an 'armed attack', as was done by the ICJ in *Nicaragua*.[48] Although the list is narrow in that it only provides examples of aggression where traditional weapons exerting physical force are used, Article 2 of the Resolution details an act of aggression as holding 'sufficient gravity' - which is also a view echoed by the ICJ - stating that only the 'most grave form of use of force' is to be viewed as an armed attack.[49]

This stance is also mirrored by legal scholars and experts who worked on the Tallinn Manual. They unanimously agreed that the mere destruction, manipulation or damage of data would not constitute an armed attack. Therefore, a cyber-attack would have to consequently

[45] United Nations Report of the Secretary-General, *'Developments in the Field of Information and Telecommunications in the Context of International Security'* (20 July 2010) UN Doc A/65/154, 15.
[46] Charter of the United Nations (n 9), Article 1(1).
[47] Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (n 18) 9.
[48] *Nicaragua v USA* (n 8)
[49] ibid para. 191

result in physical damage or destruction in order to qualify as 'armed force' and thus, potentially reach the requite levels of an armed attack.[50] This viewpoint is perhaps best demonstrated when considering the Stuxnet attack against Iran's nuclear power plant in 2010, which was cited by the Tallinn Manual as being the closest instance in which a cyber-attack reached the threshold of an armed attack.[51] In following the consequence-based approach, the attack could qualify as a use of armed force, due to the physical damage the cyber intrusion caused to the nuclear centrifuges.[52] Nevertheless, due to the fact that the attack did not cause severe harm to peoples and/or property, it could not be categorised as an armed attack. However, had the superficial damage to the centrifuges escalated to a point where there was radioactive material expelled into the atmosphere, this attack would most likely have been classified as an 'armed attack', as it would have demonstrated a 'grave use of force'.

Furthermore, it is the view of the ICJ that for self-defence to be lawfully invoked, an armed attack must be launched with the 'specific intention of harming'.[53] In the context of cyber warfare, this suggests that only operations which are carried out with the grave intention of destroying or damaging persons or physical property would qualify as an armed attack.[54] Whereas on the other hand, cyber intrusions which simply cause minor disruptions to physical property, may still be characterised as 'armed force', but would nonetheless fail to qualify as an armed attack.

Notwithstanding, if a cyber-attack does indeed qualify as an 'armed attack', it is crucial that the author of the attack is identified.[55] Through attribution, a State can therefore lawfully and effectively trigger its right to self-defence. In keeping cyber-attacks in mind, the following Section will explore the issue of attribution in relation to States and non-State actors.

2. Authorship of Cyber-Attacks

a) State Attribution

Unfortunately, no clear standard of evidence exists under which a State can attribute an armed attack to another State, and therefore lawfully invoke its right to self-defence. Nevertheless, it

---

[50] Michael Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' (4th International Conference on Cyber Conflict, Tallinn, 2012) 283, 283-288.

[51] *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Michael N Schmitt edn, CUP 2013), 56. Hereinafter 'Tallinn Manual'.

[52] ibid 56, para 13

[53] *Islamic Republic of Iran v United States of America* (n 33) para 64.

[54] Yoram Dinstein, 'Computer Network Attacks and Self-Defence' in Michael Schmitt & Brian O'Donnell (eds), *Computer Network Attack and International Law* (International Law Studies, US Naval War College 2002) 105.

[55] Couzigou, 'The Challenges Posed by Cyber Attacks to the Law on Self-Defence' (n 18) 3.

is generally assumed that the graver the charge against the accused State, the higher the burden of proof is on the victim State to prove that the accused State was the author of the attack. Thus, in order to justify the use of force, the author of a cyber-attack must be identified with a great degree of confidence by the defending State.[56] Irrespective of this, several problems appear when placing this high burden of proof on victim States - especially within the context of cyber-attacks. The anonymous, expeditious and multifaceted nature of cyber-attacks are what make attributing them to an author particularly challenging, where victim States are required to - in an accurate and timely manner - trace the source of an attack (*i.e.* the computer(s) from where it originated), and establish the identity of the author, as well as who they are affiliated with.[57]

Moreover, it is only under certain circumstances in which a cyber-attack can be attributed to a State in order to invoke self-defence. According to Article 4 of the 2001 Articles of the International Law Commission (which codifies customary law on the Responsibility of States), 'the conduct of any State organ shall be considered an act of that State…'[58] Furthermore, in instances where the author of an attack was commissioned by a State to exercise government authority to conduct cyber operations on its behalf, the licensing State would be held responsible.[59] Additionally, a cyber-attack will also be imputed to a State in circumstances where the author of the attack worked under the direct control or instruction of the State, whereby the degree of control or direction the accused State asserted was considerably high.[60]

An example of the difficulty in attributing a cyber-attack to a State was demonstrated during the cyber intrusions on Estonia experienced in 2007, where the attacks emanated from 177 countries, but were allegedly orchestrated by Russia.[61] Similarly, in recent cases such as the WannaCry cyber breach on the NHS in 2017,[62] the Bangladesh Bank cyber heist in 2016,[63] and the Sony Pictures cyber hack in 2014,[64] there was reason to believe that North Korea was

---

[56] Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum' (n 39) 254-257.

[57] Tsagourias (n 35) 233.

[58] *Official Records of the UN General Assembly, Fifty-Sixth Session,* International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), Chp.IV.E1.

[59] ibid. Art 5.

[60] ibid. Art 8.

[61] Michael N Schmitt, 'Cyber Operations and the *Jus Ad Bellum* Revisited' (n 2) 569-570.

[62] Comptroller and Auditor General, Department of Health (n 6).

[63] Al Jazeera, 'Hacked: The Bangladesh Bank Heist' (24 May 2018) <https://www.aljazeera.com/programmes/101east/2018/05/hacked-bangladesh-bank-heist-180523070038069.html> accessed 23 March 2019.

[64] A Peterson, 'The Sony Pictures Hack, Explained' *The Washington Post* (18 Dec 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.471ed546b047> accessed 17 March 2019.

the licensing State of these attacks.[65] In all of the aforementioned cases, there remained no high degree of confidence with which the victim States could attribute the perpetrating States in question, and consequently, no concrete self-defence action could be taken in these instances.

b) Non-State Actors

Notwithstanding, it is often expected that most cyber-attacks will be perpetrated by non-State actors.[66] Nevertheless, it remains unclear whether under contemporary international law, there remains a right to invoke self-defence action against such entities. In particular, Article 51 of the UN Charter neither expressly permits, nor prohibits, the use of force in these instances.[67] This has been approached by the ICJ in varying degrees, where on the one hand, it stated that the Article 51 right to self-defence was only reserved to be used against other States,[68] whereas in another case, the court refrained from commenting on whether an armed attack committed by a non-State actor would trigger the right to self-defence.[69]

State practice and *opinio juris* are also inconsistent in this area. This was demonstrated during the US's offensive actions in 2001, which remained largely uncontested by the international community, despite such action being used against the Taliban and Al-Qaeda, as opposed to the State of Afghanistan.[70] A similar stance was also taken by the international community during the Israeli military operation in 2006, where Israel declared its offensive action as only being a response to Hezbollah, and not the State of Lebanon.[71] The reliance on the right to self-defence was accepted by States in this instance too.[72] Despite this, there have been numerous instances where the international community has refrained from recognising self-defence action against a non-State actor, where State attribution could not be established.[73] It is also worth noting that, recently, there have been several attempts by Global South nations to highlight the

---

[65] Kadhim Shubber & Demetri Sevastopulo 'US Accuses North Korea over Global Cyber Crime Wave' *Financial Times* (6 Sep 2018) <https://www.ft.com/content/91453da8-b1de-11e8-99ca-68cf89602132> accessed 23 February 2019.

[66] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001-2002) 34 NYU Journal of International law and Politics 57, 58-59.

[67] *Nicaragua v USA* (n 8) para 231.

[68] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) [2004] ICJ Rep 136, para 139.

[69] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep 14, para 147.

[70] Christine Gray, *International Law and the Use of Force* (3rd edn, OUP 2008) 204.

[71] Identical letters to the UN from the Permanent Representatives of Israel, addressed to the Secretary-General and the President of the UN Security Council (12 July 2006) UN Doc S/2006/515.

[72] Raphael van Steenberghe, 'Self-defence in Response to Attacks by Non-State Actors in the Light of Recent State Practice: A Step Forward?' (2010) 23 Leiden Journal of International Law 183, 193.

[73] Christian Tams, 'The Use of Force against Terrorists' (2009) 20 EJIL 359, 379-381.

flaws which are present within the very mechanism under which States can contest matters of fundamental importance, which in this instance involves legal interpretations of Article 51 and the use of force in international law. This is primarily attributed to the procedural inefficiency and lack of transparency of the UN Security Council. For example, Mexican diplomat Pablo Arrocha Olabuenaga has voiced these concerns, stating that there are limitations in terms of how all States can equally engage and participate in public discussions on such matters, arguing that the assumed silence of States does not necessarily equate to acceptance of expansive legal interpretations on self-defence and the use of force.[74]

However, it could still be argued that State practice and *opinio juris* has recently shifted towards an emerging norm where there is a growing acceptance of the use of force against non-State actors for the purposes of self-defence.[75] This is perhaps seen most strikingly during the international military intervention against ISIL in 2014, where the overwhelming majority of States approved of this action.[76] Upon analysis however, it can be suggested that through State practice and *opinio juris,* there is still no clear indication of there being an absolute acceptance of the use of force, for the purposes of self-defence, against non-State actors. Despite some States arguing and acting otherwise, it is evident that customary law has not yet expanded in this area.[77] This has been evidenced recently when considering the perspective of Global South Nations — for instance, Brazil has continuously contested the idea of the use of force in self-defence against non-State actors.[78]

---

[74] Pablo Arrocha Olabuenaga, 'An Insider's View of the Life-Cycle of Self-Defense Reports by U.N. Member States: Challenges poses to the International Order' (*Just Security*, April 2 2019) <https://www.justsecurity.org/63415/an-insiders-view-of-the-life-cycle-of-self-defense-reports-by-u-n-member-states/?fbclid=IwAR2k5o1FAssEkEVmVY9CVimsZP-b87TDi19UP-fF0t5Hr0hJQzhpVHy4fE4> accessed 19 March 2020.

[75] See generally, UNSC Res 2249 (20 November 2015) S/RES/2249 and specifically para 5 which calls upon Member States to 'take all necessary measures' in compliance with international law to prevent and suppress acts of terrorism.

[76] Michael Scharf, 'How the War Against ISIS Changed International Law' (2016) 48 Case Western Reserve Journal of International Law 1, 20-24.

[77] Gray, *International Law and the Use of Force* (n 13) 210.

[78] Patrick Luna, 'Remarks by Patrick Luna' (2018) 112 Proceedings of the American Society of International Law (ASIL) Annual Meeting 50. For further reading see: Kevin Jon Heller, 'The Absence of Practice Supporting the "Unwilling or Unable" Test' (*Opinio Juris,* 17 Feb 2015) <http://opiniojuris.org/2015/02/17/unable-unwilling-test-unstoppable-scholarly-imagination/> accessed 18 March 2020; Statement by HE Ambassador Mauro Vieira, Permanent Representative of Brazil to the UN, addressed to the President of the UN Security Council, 'Upholding international law within the context of the maintenance of international peace and security' (17 May 2018) <https://drive.google.com/file/d/15CWYwX_G9K610xBWb7JmKelCOY-HZDKSX/view?fbclid=IwAR1RI14CkutiE1UFLVs3Ib7XQJb6ys218mziBu4ztk-ZX0kb5DH3S_cWYi4> accessed 20 March 2020; Alonso Gurmendi, 'State Practice regarding Self-Defence against Non-State Actors: An Incomplete Picture' (*Opinio Juris,* 17 Oct 2018) <http://opiniojuris.org/2018/10/17/state-practice-regarding-self-defence-against-non-state-actors-an-incomplete-picture/> accessed 18 March 2020.

Furthermore, Article 51 can be interpreted as being written with only States in mind. This restrictive interpretation can be employed when considering Article 51 in conjunction with the Charter as whole, where most of its provisions are targeted directly towards member States, where there is no mention of non-State actors. This suggests an intentional omission, where in failing to address or mention non-State actors, the Charter intends on limiting the use of force against them.[79] Therefore, it can be asserted that the right to self-defence cannot be triggered in instances where a cyberattack has been carried out by a non-State actor.

3. Cyber-Attacks and the Law of Self-Defence

In hindsight, it can be held that the majority of recent cyber-attacks conducted against States would fail to legally invoke the right to self-defence. This is ultimately because the attacks which were employed did not reach the requisite level of an armed attack. This was also reinforced by the technical challenges present in attributing an attack to a State, as well as the lack of protection afforded by international law against non-State actors. Nevertheless, this is not to say that self-defence action cannot be legally taken against cyber-attacks, but such action is only viable providing that the aforementioned elements discussed in this Section are met. Thus, in establishing that some cyber-attacks can invoke the right to self-defence under Article 51, focus must now be shifted towards whether the right to anticipatory self-defence can be triggered in response to a threat of a forthcoming cyber-attack. In doing so, it must be established whether, and if at all, a legitimate right to anticipatory self-defence exists under international law.

D. LEGITIMACY OF ANTICIPATORY SELF-DEFENCE

As mentioned in Section A, Article 2(4) provides a prohibition on the use of force between States. Nevertheless, an exception to this prohibition exists under Article 51 for the purposes of self-defence. The law of self-defence was developed from customary international law in the *Caroline* case, which also further established the conditions required to invoke the right to self-defence in anticipation of an armed attack which was imminent.[80] However, there remains much debate around whether anticipatory self-defence is accepted under international law, with questions arising around its compatibility to the law of self-defence found under Article 51 of the Charter.

1. Interpretation of Article 51 in Conjunction with the Caroline Doctrine

[79] Gray, *International Law and the Use of Force* (n 13) 207.
[80] ibid 170.

a) Restrictive Approach

From textual analysis, it is evident that there is no explicit language which incorporates the notion of anticipatory self-defence within Article 51. Furthermore, in reading the article narrowly, the right to self-defence can only be invoked 'if an armed attack occurs', therefore, it can be suggested that an armed attack must have already taken place in order for a State to rely on self-defence. Accordingly, some scholars hold that such an interpretation of Article 51 is appropriate considering that, as the prohibition on the use of force is a fundamental aspect of international law, it is likely that the drafters of the Charter wished to restrict the scope of permissible uses of force, where possible.[81] This line of reasoning is also demonstrated when observing Article 21 of the International Law Commission's Articles on State Responsibility which holds that the 'wrongfulness of an act of a State is precluded if the act constitutes a lawful measure of self-defence taken in conformity with the Charter'.[82] This is further catapulted by the view taken by many scholars that Article 51, in conjunction with Article 2(4), is exhaustive.[83] Therefore, in adopting this approach, it appears that Charter law does not extend the scope of self-defence to include anticipatory self-defence, permitting only what is explicitly expressed within it.

b) Permissive Approach

Nevertheless, it was stated in *Nicaragua* that both customary and Charter law exist in parallel, where neither sources of international law supersede one another.[84] This is also demonstrated in the opening phrase of Article 51, which refers to an 'inherent right' to self-defence, suggesting that the Charter also implicitly incorporates the doctrine of anticipatory self-defence. Therefore, as maintained by several scholars, the permissive approach illustrates that there exists a customary right to self-defence which is above and beyond the specific provisions laid out in Article 51 which only refers to scenarios where an armed attack has already occurred. Thus, in using the term 'inherent', the Charter is seen to supplement customary law, allowing for efficient governance of both individual and collective self-defence.[85] Consequently, it can be held that Article 51 does not disrupt the historic, international doctrine of anticipatory self-

[81] Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart 2010) 407- 411.
[82] *Official Records of the UN General Assembly, Fifty-Sixth Session* (n 58).
[83] Brownlie (n 25) 112-13.
[84] *Nicaragua v USA* (n 8) paras 172-178.
[85] ibid para 176.

defence, but essentially, consolidates its place in international law by providing it with dual existence under both Charter and customary law.

2. State Practice and Opinions Adopted by UN Organs

Notwithstanding, the ICJ has often shied away from expressing its view on the notion of anticipatory self-defence. For example, in *Nicaragua*, the issue of anticipatory self-defence was not raised by either party of the case, and therefore, it was expressed by the ICJ that an opinion on this matter would not be provided.[86] A similar approach was also taken by the ICJ in the *Armed Activities* case.[87] Moreover, academics who challenge the legality of anticipatory self-defence ascertain that State practice too, does not demonstrate approval of this doctrine.[88] This is mainly as a result of the technicalities associated with anticipatory self-defence, where the threshold for 'imminence', and the window in which a State is permitted to use force, is difficult to determine. This, as viewed by some academics, is arguably seen in the *Caroline* case, where the threat of an armed attack was considered as ongoing, rather than imminent.[89]

In contrast, UN reports have highlighted that despite the restrictive wording of Article 51, anticipatory self-defence is not only 'long established' but is also covered completely under the article.[90] This line of reasoning can also be applied when observing State practice and *opinio juris*. For example, in the Third Arab-Israeli War of 1967, where Israel attacked Egyptian airbases after signs that Egypt wished to attack Israel, the actions of Israel arguably demonstrated a situation where anticipatory self-defence was - and could be - relied upon.[91] Similarly, the US has often looked towards the doctrine of anticipatory self-defence to legitimise their international uses of force, as seen during its campaign against Libya in 1986,[92] and perhaps most notably, in its offensive action in Afghanistan in 2001.[93] Likewise in 2017, it was made evident in a speech given by the UK's Attorney-General that anticipatory self-defence was endorsed as a justifiable legal position to adopt in instances involving an imminent threat of an

---

86 ibid para 166.
87 *Democratic Republic of the Congo v Uganda* (n 69) 168, 222.
88 UNSC Res 487 (19 June 1981) S/RES/487.
89 Elizabeth Wilmshurst, 'The Chatham House Principles of International Law on the Use of Force in Self-Defence' (2006) 55 International and Comparative Law Quarterly 963, 964-965; *The Caroline case* (n 41).
90 United Nations Report of the Secretary-General, *In larger freedom: towards development, security and human rights for all* (2005), UN Doc A/59/2005, para 124.
91 Gray, *International Law and the Use of Force* (n 13) 171.
92 Tams (n 73) 372.
93 Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council (7 October 2001) UN Doc S/2001/946.

armed attack.[94] This explicit approval adds to the notion that the majority of States believe that this form of self-defence is lawful in exceptional circumstances where an armed attack is deemed imminent.[95]

Additionally, the actions of the UN Security Council also suggest an implicit approval of the view that Article 51 enables States to invoke the right to anticipatory self-defence in certain scenarios. This was demonstrated when it widely condemned the actions of Israel in its attack against an Iraqi nuclear reactor in 1981, stipulating that it did not fulfil the requirement necessary for triggering the right to anticipatory self-defence.[96] A similar approach was also taken in 2004 by the UN Secretary-General's 'High-Level Panel Report on Threats, Challenges and Change', where it held that anticipatory self-defence was lawful under international law, provided that the 'threatened attack is imminent'.[97] It distinguished it from instances where the threat is not imminent, but still real, by giving the example of a State acquiring the ability to procure nuclear weapons, where the hostile intent demonstrated, arguably showed a real, yet non-imminent threat.[98] Hence, although the ICJ is often reluctant in explicitly commenting upon the legality of anticipatory self-defence, the majority of UN organs show an acceptance towards this doctrine.

Therefore, it can be definitively held that when observing both State practice and the approaches adopted by UN organs, the right to anticipatory self-defence is seen to be deeply entrenched in international law, where it has dual existence under both Charter and customary law. The prevailing view reinforcing the legality of this doctrine allows States to exercise it in response to an imminent threat of an armed attack, which can thus, also be applied to the context of cyber warfare.

3. Pre-Emptive and Preventative Self-Defence

Many legal scholars have also opined that under the umbrella of anticipatory self-defence, exists two other types of self-defence, namely, pre-emptive and preventative self-defence.[99] Under pre-emptive self-defence, States can resort to the use of force for the purposes of removing

---

[94] Dapo Akande, 'The UK Attorney-General on the Modern Law of Self-Defence' (*EJIL: Talk!*, 11 January 2017) <https://www.ejiltalk.org/the-uk-attorney-general-on-the-modern-law-of-self-defence/> accessed 20 February 2019.

[95] Nevertheless, there is lack of clarity around the term 'imminence', which will be analysed further in Section D.

[96] UNGA Res 41/38 (20 November 1986) UN Doc A/RES/41/38.

[97] United Nations Report of the Secretary-General, *The Report of the UN High-Level Panel on Threats, Challenges and Change* (2004), UN Doc A/59/565, paras 188-192.

[98] ibid 189.

[99] Alex Potcovaru, 'The International Law of Anticipatory Self-Defense and US Options in North Korea' (*Lawfare*, August 8 2017) <https://www.lawfareblog.com/international-law-anticipatory-self-defense-and-us-options-north-korea> accessed 23 March 2019.

a non-imminent threat, basing this on the opponent's specific, tangible actions which are assumed to indicate the formation of a potential armed attack.[100] Therefore, the armed attack in question is in distant proximity compared to the timeframe adopted by anticipatory self-defence. The biggest proponent of pre-emptive self-defence is the US, where it used military action against Iraq in 2001 to allegedly prevent the development of weapons of mass destruction, which the US believed, may be used against them.[101] The US asserted that the recourse to armed force is permitted 'even if uncertainty remains as to the time and place of the enemy's attack'.[102] It further argued for the element of 'imminence' to be adapted to the capabilities and aims of modern adversaries.[103] This view essentially illustrates a redefinition of anticipatory self-defence, where the boundaries of what constitutes an 'immediate' and 'imminent' armed attack have shifted. Issues arise with such a reinterpretation, and is therefore, rejected. It prevents any objective evaluation of self-defence claims, as it provides States with the discretion to exercise the use of force in instances where it is uncertain when (or even whether) there is an actual threat of an armed attack. Furthermore, approval of this doctrine has not been expressed by the majority of States, and thus, fails to find its place under international law.[104]

Similarly, preventative self-defence too is a controversial aspect of international law. It is distinct from pre-emptive self-defence in that it aims to forestall the emergence of any activity pertaining to the materialisation of a threat of an armed attack.[105] Therefore, action is taken to impede the capabilities which the adversary possesses, and are usually executed before the adversary has even begun preparing for an attack.[106] This doctrine is not only disapproved by those who take a permissive approach to the *Caroline* doctrine, but also by States, who unequivocally reject any self-defence doctrine which eliminates the requirement of 'imminence'.[107]

---

[100] United Nations Report of the Secretary-General (n 97).

[101] George Bush, *The National Security Strategy of the United States of America* (2002), 13–16. <https://2009-2017.state.gov/documents/organization/63562.pdf> accessed 8 February 2019

[102] ibid 15.

[103] ibid 1.

[104] United Nations Report of the Secretary General (n 97) para 189ff; UNSC Res 487 (n 88) para 125. The latter two reports suggest that in the case of a non-imminent threat, recourse to the use of force should only be provided to the Security Council.

[105] Aiden Warren & Ingvild Bode, *Governing the Use-of-Force in International Relations: The Post 9/11 US Challenge on International Law* (Palgrave Macmillan 2014) 24.

[106] ibid.

[107] Kevin Jon Heller, 'Why Preventive Self-Defense Violates the UN Charter' (*Opinio Juris,* 7 March 2012) <http://opiniojuris.org/2012/03/07/why-preventive-self-defense-violates-the-un-charter/> accessed 23 March 2019; Similarly, see Institute de Droit International, 'Present Problems of the Use of Force in International: A.

In establishing the legitimacy of anticipatory self-defence, it can be held that States have the legal right to protect themselves against an imminent armed attack. However, there remains insufficient commentary on what constitutes as 'imminent' and whether this theoretical element of anticipatory self-defence can be applied to the practical reality in which offensive cyber weapons are both developed and utilised. Hence, we must now look towards the lawful, practical exercise of self-defence when invoked in response to a manifested and unequivocally imminent threat of a cyber-attack.

E. THE ISSUE OF 'IMMINENCE' IN CYBER-ATTACKS

In order to ascertain the temporal standard of 'imminence' within the context of cyber-attacks and anticipatory self-defence, various interpretations of the term must be considered. The two approaches which will be analysed here are the traditional and broader interpretations of 'imminence'.

1. Traditional Interpretation of 'Imminence'

Within academic literature, a singular definition of 'imminence' does not appear when determining it within the context of an armed attack.[108] However, the criteria set forth by the American Secretary of State during the *Caroline* case is often relied upon in ascertaining when preventative action by a State can be taken, confining it only to instances where the necessity of self-defence is, 'instant, over-whelming, leaving no choice of means, and no moment for deliberation'.[109] Therefore, numerous scholars have asserted that in order for an attack to be 'imminent', the force exerted by the victim State must happen just as the attack is to be launched.[110] This narrow interpretation of *Caroline* generates a high threshold for imminence, imposing a restrictive timeframe under which States can act for the purposes of self-defence.

In reality however, this interpretation is seldom applied in such a literal sense. Based on State practice, it can be seen that on the basis of credible intelligence, anticipatory self-defence is resorted to even in instances where a foreseeable armed attack is not initiated

Self-defence' (10A Resolution, Sesion de Santiago, 27 October 2007) para 6: 'There is no basis in international law for the doctrine of "preventative" self-defence in the absence of an actual or manifestly imminent armed attack'. <http://www.idi-iil.org/app/uploads/2017/06/2007_san_02_en.pdf> accessed 4 May 2020.

[108] Noam Lubell, 'The Problem of Imminence in an Uncertain World', in M Welled (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 697, 711.

[109] *The Caroline case* (n 41); Gray (n 13) 157-158

[110] Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1998-1999) 37 Columbia Journal of Transnational Law 885, 930.

minutes, or even hours, beforehand.[111] Examples of this are illustrated through the actions of the US in 2001, where its military intervention in Afghanistan was formulated with the primary intention of thwarting future terrorist attacks by al-Qaeda, rather than to stop armed attacks which were on the cusp of materialisation.[112] Likewise, the UK, who was an ally of the US in 2001, expressed that such action was necessary to 'avert the continuing threat of attacks'.[113] Therefore, there is clear contention between the practices of some States, and the traditional approach towards the *Caroline* principle, where it is often held that an armed attack need not occur in the immediate future in order to invoke self-defence.[114]

A similar approach to the aforementioned is also supported by various academics, where the high temporal standards of the *Caroline* principle are thought to deprive States the opportunity to adequately react against potential attacks, inevitably leading them to fail in protecting their territory from inconceivable degrees of harm.[115] Ultimately, in confining the timescale under which States can respond, the objective and purposes of the right of self-defence are defeated. This is especially relevant in instances where there is no time for a peaceful resolution and the relationship between the parties have deteriorated drastically.

2. Suitability of the Traditional Interpretation in a Cyber Context

This strict standard on temporal imminence is unsuitable within the context of contemporary warfare, where technological advancements have helped to catalyse threats which are both expeditious and unprecedented in nature, making traditional approaches to the use of force and self-defence inadequate. This is especially evident in the context of cyber-attacks, where in following this restrictive approach towards 'imminence', States would be required to act just before an adversary is about to press the button of a pre-written code that would launch a cyber-attack.[116] The immediate and fast-paced nature of cyber-attacks would make this impossible, as once they are executed, the time taken for the pre-written code to reach the target State is negligible, thus precluding any ability to stop the cyber operation, by relying on anticipatory

---

111 Terry Gill, 'The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy' in M N Schmitt and J Pejic (eds), *International Law and Armed Conflict: Exploring the Faultiness* (Martinus Nijhoff Publishers 2007) 129-139.

112 Gray, *International Law and the Use of Force* (n 13) 200-202.

113 Letter dated 7 October 2001 from the Chargé d'affaires ai of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the President of the Security Council (7 October 2001) UN Doc S/2001/947.

114 Gray, *International Law and the Use of Force* (n 13) 250–253.

115 Dominica Svarc, 'Redefining Imminence: The Use of Force Against Threats and Armed Attacks in the Twenty-First Century' (2006) 13 ILSA Journal of International & Comparative Law 171, 184.

116 Hayward (n 14) 414.

self-defence.[117] This can be likened to a situation where one would have to react immediately before an individual were to press the trigger button of a bomb which they were carrying.[118] The rejection of this traditional interpretation is also supported by the majority of experts behind the Tallinn Manual.[119]

However, relaxing the strict interpretation of 'imminence' is often met with some resistance, especially as under international law, States are not (and should not be), provided with complete freedom to exercise aggression for the purposes of self-defence.[120] Additionally, it can be argued that using self-defence in response to an armed attack which is not immediately forthcoming is inadequately supported by State practice and *opinio juris*, thus having no definitive place under customary law.[121] Nevertheless, it is the view of the present author that it would be illogical to afford such a high standard of temporal imminence to instances involving potential cyber-attacks, as in that case, States would be unable to adequately stall them due to the limited timeframe under which they are required to act.

Alternatively, it may be more appropriate to move away from the traditional approach put forth by the *Caroline* doctrine. In adopting a broader interpretation of 'imminence', which has been accepted by States such as the US and the UK, the law of self-defence would reflect the realities which are present in contemporary warfare today. However, there must also be a strict and objective criterion agreed upon prior to any reinterpretation of 'imminence' being made, so as to avoid excessive and arbitrary uses of force veiled by the justification of self-defence.

3. Broader Interpretation of 'Imminence'

Some academics have endorsed that the appropriate test for determining when the right to anticipatory self-defence can be invoked is whether or not the last possible window of opportunity to block an armed attack has been presented.[122] As specified by the Tallinn Manual, this window 'may present itself immediately before the attack in question or, in some cases, long before it occurs.'[123] The expansion of the traditional approach therefore allows States to act in self-defence even when a prospective attack does not pose an immediate threat. However, it can

[117] ibid.
[118] ibid.
[119] Tallinn Manual (n 51) 65.
[120] Irene Couzigou, 'The Fight Against The "Islamic State" in Syria: Towards the Modification of the Right to Self-Defence?' (2017) 9 Geopolitics, History, and International Relations 80, 92.
[121] UNGA Res 60/1, World Summit Outcome (24 October 2005) UN Doc A/RES/60/1, para 79.
[122] Hayward (n 14) 414-426.
[123] Tallinn Manual (n 51) 65.

only be adopted if it is in accordance with the terms, principles and purposes of both customary and Charter law.[124] Furthermore, any preventative action taken by the victim State must be based on well-sourced, credible intelligence, as well as other 'relevant' factors.[125] Essentially, these other 'relevant' factors can be utilised in making a calculation on the timeframe within which a State can launch an attack for self-defence purposes, lest it is too late. Unfortunately, there is lack of clarity on what the aforementioned factors may be. However, in observing the approaches taken by both the US and the UK, a combination of non-exhaustive factors seem apparent in determining the imminence of an attack, and thus estimating the window of opportunity in which a State can resort to self-defence. These factors are detailed below:

a) *Nature of the Threat*

Firstly, an assessment must be made on the specific nature of the threat considering, the type of weaponry used (traditional kinetic weapons or non-conventional, technological weapons); the magnitude of the potential harm it could cause; and the time in which it is likely that the attack will be launched.[126] These factors can help to determine whether the damage/destruction the threat could cause is something which could be effectively prevented by the target State. Therefore, the attack must not only be serious enough to rise to the requisite level of an armed attack, but its materialisation must also be made highly probable, if not certain, if no action is taken by the target State to stop it. Ultimately a State can then evaluate the proximity of the threat in relation to the timeframe under which it can react to prevent harm from taking place.

b) *Capabilities of the Opponent*

Additionally, the victim State must consider the capabilities of the alleged opponent.[127] This can help to determine the likelihood of the attack being realised, and therefore, the probability of the potential attack succeeding. Consequently, this will enable States to ascertain whether preventative action is at all necessary for the purposes of self-defence. In understanding the offensive capabilities which the opponent possesses, a State can also estimate the last possible window of opportunity for when self-defence can be triggered, where if a State were not to act within this time, it would lose the opportunity to effectively protect itself.[128]

c) *History of Hostility*

---

[124] Tams (n 73).
[125] UN Doc S/2001/947 (113) 184.
[126] Hayward (n 14) 414.
[127] ibid 417-427.
[128] ibid.

Consideration may also be given to instances where there is/has been a pattern of coordinated armed military action against the defending State, which can help to further reinforce the belief that a potential attack may be underway.[129] A continuous history of hostility towards the defending State can, therefore, also demonstrate the specific hostile intent of the alleged adversary, which is a requirement under international law to invoke self-defence.

d) *Exhaustion of All Viable Non-Military Remedies*

Furthermore, it is necessary that the defending State has exhausted all other alternatives to the use of force in remedying the hostile situation present, where it has no other means possible than to resort to self-defence.[130] In order to lawfully invoke the right to self-defence, consideration of this factor is particularly important, especially in instances where the forthcoming attack is not necessarily immediate. This is because the primary purpose of international law is to maintain international peace and security, which includes limiting the use of armed force where possible.

e) *Suitability of the Broader Interpretation in a Cyber Context*

In observing the above factors, States can determine not only whether there is a strong need for offensive action, but also the last practical window in which they can act for the purposes of anticipatory self-defence. Academics, as well as the Tallinn Manual, have endorsed this broadened interpretation of 'imminence', arguing that it allows States the possibility under international law to effectively defend themselves against cyber-attacks which are likely to occur in the future.[131] As mentioned previously in relation to the traditional approach, a broadened interpretation of 'imminence' is necessary due to the expeditious nature of these attacks, as once a cyber-attack is about to be launched, it is unlikely that States would be able to realistically prevent them.

It could also be argued that this approach towards 'imminence' does not necessarily move away from the ordinary understanding of the word, where an 'imminent' act can be one which is either presently underway (and therefore 'immediate'), or one which is impending, in which case it is separated by space and time.[132] Thus, in terms of anticipatory self-defence, an 'imminent' attack can be one which presents itself immediately, or in some instances, long

[129] Terry Gill and Paul Ducheine, 'Anticipatory Self-Defense in the Cyber Context' (2013) 89 International Law Studies (US Naval War College) 438, 466.
[130] ibid 449.
[131] Hayward (n 14) 414-416
[132] *Black's Law Dictionary* (6th edn, St Paul Minn West Publishing Co. 1990) 749, 750.

before it is identified. Therefore, the restrictive interpretation of *Caroline* seems more analogous with instances that present only an immediate threat of an armed attack. This overlooks other instances which could also be logically defined as 'imminent'. Moreover, in following this broadened interpretation, States are still required to adhere to a temporal standard which is restrictive to some degree, as they are only permitted to resort to self-defence in the *last* possible window of opportunity in which they could thwart a potential armed attack. Nevertheless, in straying from the traditional understanding of 'imminence', there is a possibility that some States may misuse the protection this interpretation offers. Through exercising their right to anticipatory self-defence, even in instances where the proximity of an attack is not in the near future, States could possibly use armed force for entirely self-serving purposes on the basis of unreliable intelligence and mere speculation. This would be counterintuitive to the aims and purposes of international law.

Moreover, instances such as these appear to be reflective of States exercising preventive self-defence, where they would seek to halt the progression of a future attack, despite having no accurate information on when such an attack may occur, or any incontrovertible evidence against the perpetrating State. As analysed in Section C, such defensive action is considered illegitimate by the majority of States, and therefore, is illegal under international law. By the same token, some legal scholars have proposed that this approach towards temporal imminence could also mirror pre-emptive, as opposed to anticipatory self-defence. As discussed in Section C, pre-emptive self-defence gives States the scope to act within a longer time horizon, in which they can interpret the tangible actions of the opponent State as being consistent with the development of an armed attack. In other words, under these circumstances, the defending State is permitted to act against a non-imminent threat. However, pre-emptive self-defence too, does not currently find its place under international law.

Notwithstanding, the only way in which a State can legally justify its actions under anticipatory self-defence, and by extension, protect itself effectively from a forthcoming cyber-attack, is through adopting the broadened interpretation of 'imminence', in which the 'last possible window' test is employed. Therefore, if we are to consider this approach, it is crucial that there is broad agreement across the international community on the factors which should be taken into consideration when determining imminence, and that the evidence gathered against the author of a potential attack is incredibly compelling. Ergo, the burden of proof on the victim State in this regard must be high for it to justify the use of anticipatory force for the purposes of self-defence, thus helping to preserve overall international peace and security. However,

affording such a high burden of proof onto victim States may be challenging, especially in the context of cyber-attacks, as it is not only difficult to identify the author of such operations as discovered in Section B, but also because in practice, it is more challenging to acquire sound intelligence pertaining to when an armed attack will happen, as opposed to when an attack is already underway.[133] Hence, it must be analysed whether this broadened interpretation to 'imminence' can be applied to the operational reality under which a potential cyber-attack can be detected, therefore allowing the right to anticipatory self-defence to be invoked in these instances.

F. PRACTICAL APPLICATION OF ANTICIPATORY SELF-DEFENCE IN A CYBER CONTEXT

In order to invoke the right to anticipatory self-defence within the last window of opportunity, a State must be able to identify a cyber-attack during its development phase. It is often assumed by scholars that States are unlikely to know when a cyber-attack is coming due to the short interval between the time in which it is launched and the time taken to reach the target.[134] This immediately throws off any question relating to anticipatory self-defence, because if a State were unable to detect a cyber-attack during its planning phase, it would be unable to perform an analysis on its imminence.

However, this view is misguided in that it places focus on a restricted window of time, taking into account only instances where an adversary chooses to launch a cyber-attack, rather than on the fact that target States can often detect the planning of a cyber-attack far in advance.[135] The investment in resources for tackling cyber-threats, as seen for example with the creation of the US Cyber Threat Intelligence Integration Centre in 2015,[136] suggests that the quality of detection in technologically advanced States is likely to increase in the coming years. This, in effect, may allow anticipatory self-defence to be more readily employed within the context of cyber warfare.

Notwithstanding, once a State has detected activity pertaining to the planning of a cyber-attack, it is crucial to evaluate whether the broader interpretation of 'imminence', can be

[133] Hayward (n 14) 418.
[134] William Banks, 'The Role of Counterterrorism Law in Shaping ad Bellum Norms for Cyber Warfare' (2013) 89 International Law Studies (US Naval War College) 157, 183.
[135] Hayward (n 14) 419; Siobhan Gorman, 'US Plans Cyber Shield for Utilities, Companies' *The Wall Street Journal* (8 July 2010) <https://www.wsj.com/articles/SB10001424052748704545004575352983850463108> accessed 4 May 2020.
[136] ibid.

realistically applied to instances involving standalone cyber-attacks or those which are carried out in conjunction with kinetic weaponry.

1. Standalone Cyber-Attacks

As explored in Section B, cases which have involved standalone cyber-attacks have often failed to rise to the requisite level of an armed attack. Nevertheless, if a standalone cyber-attack was detected and able to qualify as an armed attack, the right to anticipatory self-defence could possibly be relied upon in these instances.

Improvement of a State's detection capabilities, as seen with the US and assumed in other technologically advanced States, suggests that it is increasingly more likely for cyber-attacks to be identified well in advance. This inevitably places focus on the issue of 'imminence', as the time between when a State learns of an adversary's intention to attack, and the moment in which such an attack will materialise, could potentially be longer than expected.[137] This is particularly relevant in the case of cyber operations which qualify as armed attacks, as cyber-attacks which have the ability to cause a significant amount of harm are usually highly customised and take longer to develop, therefore increasing the probability of them being detected in advance.[138] Consequently, standalone cyber-attacks which equate to an armed attack will rarely present themselves as 'imminent'. In other words, the last possible window under which a State is required to effectively stop such an attack, would not have yet arrived. In these instances, the principle of anticipatory self-defence is automatically negated as a justifiable use of force, with the argument being that there would still be an opportunity to effectively prevent the attack from taking place, through utilising alternatives other than armed military force.

It would therefore seem that the most likely application of the broader interpretation of 'imminence' would be in instances where cyber force is used in conjunction with kinetic weaponry. However, whether anticipatory self-defence can still be legally relied upon in these instances is a point of contention, as will be analysed below.

2. Cyber-Attacks in Conjunction with Kinetic Weaponry

[137] Hayward (n 14) 424.
[138] ibid 421-422.

Cyber-attacks which work in conjunction with kinetic weaponry are more likely to be carried out than standalone cyber-attacks, with the former gaining more prevalence over time.[139] Furthermore, as demonstrated on several occasions, most standalone uses of offensive cyber technology have not been of sufficient enough gravity to be identified as an 'armed attack'.

Accordingly, it would seem more appropriate to apply the doctrine of anticipatory self-defence to instances where cyber technology is viewed rather as an antecedent to further, more severe cyber-attacks, or as a precursor to armed attacks which employ kinetic weaponry.[140] Therefore, if established that there is evidence of an impending attack, preliminary uses of cyber force which do not qualify as an armed attack may, as a whole, rise to the level of an armed attack, if combined with kinetic weaponry or other serious cyber-attacks. Thus, anticipatory self-defence action would not be against the initial cyber-attack, but rather against the impending kinetic, or more serious, cyber-attack. Leading academics have proposed a test to help determine when a State may use anticipatory force in these instances:[141]

> (1) The cyber-attack must be part of an overall operation culminating in an armed attack;
>
> (2) the cyber-attack is an irrevocable step in an immediately imminent and most likely, unavoidable attack, and;
>
> (3) the victim State is reacting in advance and during the last possible window of opportunity available to effectively counter the attack.

Nevertheless, this approach is problematic, the reason being that, the second part of the test requires the cyber-attack to be an indicator of an 'immediately imminent' and 'unavoidable attack'. This echoes the traditional interpretation of *Caroline*, where the threat of an armed attack must be 'instant, over-whelming, leaving no choice of means, and no moment for deliberation'.[142] As explored in Section D, it is clear that the standard of imminence which this interpretation employs is far too narrow, and therefore inapplicable to a cyber context. Furthermore, using anticipatory force against an initial cyber-attack which does not rise to the level of an armed attack contradicts the customary principles of 'necessity and proportionality', as well as the general law on self-defence. This is because defensive action can (and should) only be taken against a qualified armed attack and not prematurely against instances of armed force.

---

[139] Scott Applegate, 'The Dawn of Kinetic Cyber', in K Podins, J Stinissen, and M. Maybaum (eds) *5th International Conference on Cyber Conflict, Tallinn* (NATO CCD COE Publications 2013).

[140] Horace Robertson Jr., 'Self-Defense against Computer Network Attack under International Law' (2002) 76 International Law Studies (US Naval War College) 121, 139.

[141] ibid 139-140.

[142] *The Caroline case* (n 41); Gray (n 13) 157-158

The broader interpretation of 'imminence' cannot be applied to this situation either. This is due to the fact that the last possible window in which a victim State can react has arguably not arrived, as the cyber-attack in question is only a precursor to future armed attacks, and not one itself. Furthermore, this initial use of cyber force does not in itself pose an imminent threat, therefore any action taken to thwart it is more illustrative of pre-emptive or preventative self-defence, which as discussed in Section C, is not legally recognised under international law. Therefore, in order to legally apply the 'last window' test, a victim State can only use anticipatory self-defence in response to a threat of a materialised armed attack, not against a cyber-attack which qualifies as armed force.

However, by not being able to apply the broader interpretation of 'imminence' in these situations, States may be unable to effectively react in a timely manner to protect themselves from an 'unavoidable' and 'immediately imminent' armed attack - especially as the initial cyber-attack may act as an irrevocable step leading to the materialisation of the armed attack. Nevertheless, the practical reality remains that States would be unable to legally invoke their right to anticipatory self-defence against both standalone cyber-attacks, or those which are employed in conjunction to kinetic weaponry, even if a broader interpretation of 'imminence' is adopted.

G. CONCLUSION

I have argued that under international law, anticipatory self-defence cannot be invoked in response to the threat of a cyber-attack. This firstly due to the fact that most cyber-attacks are unlikely to reach the requisite level of an 'armed attack' in order to lawfully trigger self-defence, as demonstrated by previous cases. Secondly, even if a cyber-attack were to qualify as an armed attack, States would face challenges in attributing it to a State or non-State actor - where international law does not currently allow any self-defence action against the latter.

Nevertheless, it could still be possible for a State to rely on the right to self-defence (including anticipatory self-defence), if a cyber-attack constitutes an 'armed attack' and can be attributable to a State. However, anticipatory self-defence can only be invoked in response to an imminent threat, but as explored, there remain operational difficulties in doing so. The lack of consensus amongst the international community regarding the temporal standards of 'imminence', makes it challenging to determine when, and whether, force can be used in these situ-

ations. Nonetheless, in following the broader interpretation of 'imminence', and therefore employing the 'last window' of opportunity test, States may have the ability to respond in a timely and effective manner to a potential cyber-attack.

However, the challenge in this approach is not only the high burden of proof afforded to States in justifying their anticipatory actions, but also the fact that, in practice, both standalone cyber-attacks, and those combined with kinetic weaponry, are still unlikely to fit the temporal standards of the 'last window' approach. This is notwithstanding that, in my opinion, the broader interpretation of 'imminence' may also lead to a slippery slope where States can utilise it at their own discretion, thus defeating the aims and purposes of international law. Moreover, the relaxed temporal standards under this approach appear to mirror pre-emptive, and possibly even, preventative self-defence, which is not lawful under international law.

In order to effectively mitigate the relationship between the law of self-defence and cyber warfare, it is first necessary for the international standards of attribution to be lowered.[143] This also includes international law accommodating States by providing them with sufficient protection against non-State actors, who are also the most common perpetrators of cyber-attacks. Furthermore, to invoke anticipatory self-defence, the issue surrounding the interpretation of 'imminence' must be adequately addressed. This can be achieved through obtaining broad consensus around the definition of the term and adapting it in a way which reflects the contemporary challenges posed by cyber-attacks, whilst also upholding the aims and principles of international law. After establishing agreement on the interpretation of 'imminence', it is crucial for States to develop an efficient response framework by also considering both the level of attribution and the severity of the attack. This will enable States to respond in line with the customary principles of 'necessity and proportionality'. Moreover, key decision-makers must also consider whether their response should involve kinetic or non-kinetic instruments and the degree of force they intend to employ, if necessary.[144] The appropriate response may differ depending on the situation at hand, however, the primary position taken by academics is that the response to cyber-attacks — whether potential or otherwise — should be a question of politics.[145] This may include diplomatic, economic or military measures, each response varying depending on the outcome the potential cyber-attack could cause. However, until the above

[143] This suggestion was addressed in *Prosecutor v Dusko Tadic* (15 July 1994) Judgement Appeals Chamber ICTY, IT-94-1-A, para 131.
[144] Jarno Limnéll, 'Proportional Response to Cyberattacks' (2017) 1 Cyber, Intelligence, and Security 37, 49-51.
[145] ibid; David Graham, 'Cyber Threats and the Law of War' (2010) 4 Journal of National Security, Law and Policy 87, 96-98.

changes are made, it remains realistically unviable for States to lawfully invoke this right in response to the threat of a cyber-attack.