Fountain University Law Journal (FULAJ) (2024) 1(2) 137-153
A Publication of College of Law, Fountain University, Osogbo, Nigeria
https://fountainjournals.com/index.php/FULAJ/index

CONTEMPORARY TRENDS IN CYBER WARFARE AND THE USE OF FORCE IN INTERNATIONAL LAW: DEMYSTIFYING ARTICLE 2 (4) OF THE UN CHARTER

By

Suleiman Usman Santuraki*

Abstract

The proscription of the use of force under article 2 (4) of the United Nations (UN) Charter is generally accepted as having the effect of a treaty provision as well as customary principle in international law. Interestingly, the scope and effect of article 2 (4) is still being debated. Emerging trends on the use of cyber space creates a new dimension to the argument on the scope of article 2 (4). In 2017, North Korea allegedly hacked South Korean Defence systems stealing terabytes of sensitive defence data, and was also suspected of masterminding the hacking of a US filmmakers' data base resulting in losses of millions of dollars. In response, the US allegedly engineered a devastating attack on the North Korean cyber space, and sanctioned North Korea for the hacking of Sony Pictures. Again, the US accused Russia of meddling in its electoral process largely using the cyber space, thus, imposed several sanctions on Russia. Russia also retaliated by expelling some US diplomatic staff from Moscow. Using doctrinal research methodology, this paper examines how these activities relates to the international legal regime on the use of force. It aims to establish how the occurrences of cyber warfare have influenced an emerging reinterpretation of article 2 (4). The paper relied on wide literature relating to the use of force and cyber warfare to achieve the objective of interpreting article 2 (4) in line with contemporary happenings. It argues that cyber warfare could amount to an armed attack capable of activating the right of other states to self-defence. The paper finds that states and publicists have equally treated cyber warfare as an armed attack, though determining the proportionality or necessary retaliatory actions may be a complex issue.

Keywords: **Use of Force, Cyberspace, Cyber-warfare, UN Charter, International Law.**

1.0 INTRODUCTION

The decision to proscribe the use of force in the international relations of states is one of the most innovative and bold provisions of the United Nations (UN) Charter. [1]Consequently, it has generally been the essence of international law

* LL. B, BL., PhD, Senior Lecturer, Nigerian Law School, Yola Campus, Yola Adamawa state, suleisant@gmail.com, 07030632866

that developed after the Second World War under the UN system. The importance of this prohibition is seen considering the effect it is supposed to have on inter-state relationship and international peace. This provision having been in force for more than seventy years is generally considered to have attained the status of *jus cogens* – an imperious principle of international law, which states are not permitted to derogate from.[2] The provision is considered *jus cogens* because it has been upheld by the international community as a binding and a superior rule of international law.[3] There is no doubt that the UN Charter has proscribed the use of force states via article 2 (4), or that such prohibition reflects the position under treaties and customary international law.[4] The difficulty has been in relation to the exact meaning and scope of Article 2(4).

The UN Charter was built around the essential features of statehood, reflecting the need for states to protect and defend their sovereignty and territorial integrity. Article 2(4) should therefore be understood within the context of the UN system and its primary aim. The UN Charter prohibits states from resorting to force in their international relations to assure nation states of a commitment to peace. It is also meant to guard against that which could easily imperil international peace and cohesion.

Over the past two decades, the international community has experienced rapid advancement in information and communication technology (ICT). With this advancement came the challenge of abuse of such technology.[5] Over the past decade alone, there have been several cyber-related attacks on nations, national infrastructure, and private enterprises across several nations. This include, among others, the Estonian case,[6] the disruption of cyber activities in Georgia,[7] the attack on Iranian atomic amenities,[8] to the more recent attack on Sony pictures in the US and the alleged counter attack on North Korea.[9] In addition, the unravelling facts behind the alleged use of social media and the internet by

[1] Michael Wood, 'The Law on the Use of Force: Current Challenges', *Singapore Year Book of International Law and Contributors* {2007} (Vol. 11): 1–14.

[2] C*ase Concerning Military and Paramilitary Activities in and Against Nicaragua (Merits),* ICJ Reports (1986). 14, para. 190. (*the Nicaragua case*).

[3] See Evan J. Criddle and Evan Fox-Decent, 'A Fiduciary Theory of Jus Cogens', *Yale Journal of International Law*, {2009} (vol. 34) (No. 2) 331–87, 331. See also, ibid.

[4] C*ase Concerning Military and Paramilitary Activities in and Against Nicaragua (Merits),* ICJ Reports (1986). 14, para. 176. (*the Nicaragua case*).

[5] C. Demchak, 'Resilience, Disruption, and a Cyber Westphalia: Options for National Security in a Cybered Conflict World', in N. Burns and J. Price (eds), *Securing Cyberspace: A New Domain for National Security*, 2012; J.S. Nye Jr., *Normative Restraints on Cyber Conflict*, (Belfer Center for Science and International Affairs, 2018).

[6] Russia accused of unleashing cyberwar to disable Estonia, The Guardian, Thursday 17 May 2007. https://www.theguardian.com/international. Accessed 12/13/2017.

[7] Miroslav Mareš & Veronika Netolická, Georgia 2008: Conflict Dynamics in the Cyber Domain, Strategic Analysis, {2020)} 44:3, 224-240, DOI: 10.1080/09700161.2020.1778278. see also, UK says Russia's GRU behind massive Georgia cyber-attack, https://www.bbc.com/news/technology-51576445, Accessed 11/25/2020.

[8] Jonathan Fildes, 'Stuxnet Worm 'Targeted High-Value Iranian Assets', BBC News, 23 September, 2010, www.bbc.com/news <Accessed 14/12/2017>.

[9] BBC, 'The Interview: A Guide to the Cyber Attack on Hollywood', BBC News, 29 December, 2014, www.bbc.com/news <Accessed 11/12/2017>.

Russia to influence the 2016 US Presidential elections adds to the dilemma.[10] The sanctions and counter sanctions that followed this incident complete the picture depicting a contemporary challenge that needs to be addressed.

Because international law regime on the use of force was developed in an era when the current trends in technology would not have been realistically anticipated, it has become difficult to fit them into the existing legal framework. For one thing, the prohibition on the use of force has always been interpreted to focus on the military or armed forces. Thus, considerations of other possibilities such as economic and political coercion have been overwhelmingly dismissed.[11] This being the case, where does cyber warfare fit in? Can we afford to dismiss all the real and potential uses of cyberspace by states to pursue aggressive national agendas especially when it clearly targets other states? Where it is aimed at destroying the economy of other states? Where it is aimed at manipulating the political structure of other states? Where it is aimed at military facilities and infrastructure of other states?

This paper examined the essence of the prohibition under article 2(4)[12] as one aimed to protect the sovereignty, political independence, and integrity of all states weak and strong. It attempted to demystify article 2(4) by interpreting it in line with contemporary reality to proscribe any activity that violates the spirit of the prohibition against the use of force and the UN Charter in general.[13] It discussed the attribution of cyber-attacks to states, in the face of activities shrouded in doubt and cover-ups as most recent cyber-attacks on states or their facilities have been carried out through private individuals. It also analysed the right of states to self-defence under article 51 of the UN Charter and how states may respond to such attacks.

2.0 RECENT TRENDS IN CYBER WARFARE

As the international community become more reliant on the cyberspace and related technological advancement, it has become easier for states and individuals to use it towards achieving skewed objectives.[14] Contemporary realities indicate that the Cyberspace is capable of being used for as many, if not more purposes as desired. States now resort to achieving their hitherto proscribed objectives using complex technology to undermine the economic, political, and military advancement of other states. And that is easily achieved with less political risk due to the out of kilter nature of such actions.[15]

---

[10] Office of the Director of National Intelligence, 'Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution,' 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf%0A<accessed 15/12/2017>

[11] See for example, Jozef Valuch, Tomáš Gábriš, and Ondrej Hamuľák, 'Cyber Attacks, Information Attacks, and Postmodern Warfare,' *Baltic Journal of Law & Politics,* [2017] (10) (1) 63–89, 207.; See also United Nations, 'Charter Of The United Nations' (San Francisco, 1945), doi:ISBN: 9789210020251, preamble, para 7.; Albrecht Randelzhofer and Oliver Dorr, 'Article 2 (4),' in Bruno Simma and others (eds), '*The Charter of the United Nations',* (3rd edn , Oxford: Oxford University Press, 2012), 209.; James A. Delanis, 'Force under Article 2(4) of the United Nations Charter: The Question of Economic and Political Coercion' *V and. J. Transnat'l L,* {1979}, (vol. 12), (no. 101) 132.; (n 2, p 73).

[12] United Nations, ibid.

[13] For argument along the same line, See (n 2), 73.

[14] (n 11).

[15] Albrecht Randelzhofer and Oliver Dorr, Article 2 (4): in *The Charter of the United Nations*, Bruno Simma and others (eds), (3rd ed. Oxford University Press, 2012). 40.

Contemporary trends in cyber-attacks can be categorised into two broad classes for the purposes of this paper. These include information warfare and cyber warfare.[16] Information warfare basically comprises of using the cyberspace to promote propaganda, to disfigure websites, to execute Distributed Denial-of-service (DDoS) campaigns, to leak vital information, and to pursue innovative cyber surveillance.[17] The objective could be to downgrade a state's ability to respond to attacks, to cause economic or other related damage, or simply to influence the general political path of a dispute.[18] In most of these kinds of attack, the aim is to disrupt services and mislead or disfigure information; neither military nor civilian infrastructure is targeted. A classic example is the attack by Russian hackers on Ukrainian Cyberspace during the Russian conflict with Ukraine 2013 - 2016.[19] Cyber warfare on the other hand refers to situations of conceivable exploitation of cyberspace by states by way of direct electronic meddling with foreign military objectives intending to damage infrastructure or system. It may also include the deliberate targeting of civilian objectives which may lead to damage or undermining national system.[20]

In recent years, several states have been victims to what will qualify as cyber-attack or cyber-warfare. A rough survey over the past decade reveals several such instances cutting across different regions and of varying sophistication, objective and effect. This clearly is indicative of a global phenomenon. To start with, there was the case of overwhelming denial of service on Estonia in April 2007, a country known as being vastly reliant on computers.[21] For a period of three weeks, Estonia was under a coordinated distributed denial of service attack (DDos) which almost shut down the entire country's private as well as public sites.[22] The attacks initially targeted websites of government institutions and later financial institutions, and major media outlets in what was seen as a planned move to prevent dissemination of information regarding the attack.[23] Alarmed at the rate and sophistication of the attack, the North Atlantic Treaty Organisation (NATO) (of which Estonia is a member) described it as 'an operational security issue … which goes to the heart of the alliance's modus operandi.'[24] The attacks, though infinitely attributed to Russia, was not clearly established to have emanated from the Russian government.

Georgia was also victim of coordinated cyberattacks in 2008 which happened during an armed conflict with Russia. This attack burdened and effectually shut down targeted government websites and decelerated internet services.[25] As a result, the attack prevented government agencies from disseminating

[16] Valuch, Gábriš, and Hamuľák, (n 11)."
[17] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014). 77.
[18] Valuch, Gábriš, and Hamuľák, (n 11) 33.
[19] Valuch, Gábriš, and Hamuľák, (n 11) 33.
[20] James J Wirtz, *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, in Kenneth Geers, (ed) *Cyber War in Perspective: Russian Aggression Against Ukraine*, (vol. 3, NATO CCD COE Publications, 2015), 29–37. 67.
[21] (n 20).
[22] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia,' *The Guardian, 17 May*, 2007, https://www.theguardian.com/international. <accessed 17/12/2017>.
[23] Ibid.
[24] (n 11).
[25] (n 22).

information to citizens during a period of emergency. Like what transpired in Estonia, media organisations and private companies were also attacked. Again, though Russian was blamed, the evidence was not conclusive enough to establish responsibility. This incident accentuates the possibility and potentials of cyberwarfare as a tool of modern warfare which is relatively cheap and easy to carry out.

Most alarming of all the cyber-attacks in recent times, as far as the use of force is concerned, is the 2010 coordinated attack on Iran. This attack, described as 'one of the most sophisticated pieces of malware ever detected',[26] was designed to target Iranian nuclear reactors. The objective was to calculatingly slow down and monitor the reactors. The cyber-attack though discovered in 2010 was said to have been in place for at least over a year. Though the extent of damage was not ascertainable because of the sensitivity of the issue, the nuclear reactor was reportedly damaged.[27] This incident proves the practicability of cyber warfare resulting in physical damage to a state's sensitive defence infrastructure and potential human casualty. There were initial accusations that the United States (US) and Israel were responsible for the attack, later confirmed by sources from the US government.[28]

In 2014, a cyber-attack on Sony Pictures, an American filmmaker, crippled computers at the company and led to loss of confidential documents and data relating to movies.[29] North Korea was allegedly responsible for the attack in response to a comedy involving plots to eliminate the North Korean leader; it denied responsibility for the hack.[30] The US President vowed to respond "proportionally" to the cyber-attack on Sony pictures.[31] And true to his words, a few days after the threat by President Obama, North Korea suffered one of its worst internet crisis leading to the entire country being completely disconnected from the World Wide Web.[32] The US government declined to comment directly on the issue, though US State Department spokesman stated: "As we implement our responses, some will be seen, some may not be seen."[33]

In 2017, some North Korean hackers allegedly compromised the South Korean Defence website and made away with enormous store of classified data including wartime exigency strategies jointly designed by the United States and

[26] Jonathan Fildes, 'Stuxnet Worm 'Targeted High-Value Iranian Assets', *BBC News, 23 September*, 2010, www.bbc.com/news <Accessed 14/12/2017>.
[27] Veronika Mackova, 'Cyber War of The States: Stuxnet and Flame Virus Opens New Era of War', Policy Papers 2 (Bratislava, Slovakia, 2013), http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova.pdf <Accessed 15/12/2017>; 5.
[28] David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *The New York Times, June 1,* 2012, https://www.nytimes.com/pages/world/middleeast/index.html <Accessed 14/12/2017>.
[29] BBC, 'The Interview: A Guide to the Cyber Attack on Hollywood', *BBC News, 29 December*, 2014, www.bbc.com/news <Accessed 11/12/2017>.
[30] ibid.
[31] David E. Sanger, Michael S. Schmidt, and Nicole Perlroth, 'Obama Vows a Response to Cyberattack on Sony', *New York Times, December 19*, 2014, https://www.nytimes.com/pages/world/asia/index/html <Accessed 3/12/2017>.
[32] Nick Allen, 'North Korea Internet 'Totally Down' as US Cyber Attack Suspected' *The Telegraph, 22 December*, 2014, www.telegraph.co.uk. <accessed 28/1/2018>.
[33] Ibid.

South Korea.[34] In a similar incident earlier on, the US was alleged to have hacked into North Korean intelligence website in 2010.[35]

There were serious allegations in 2016 that Russia had used the cyberspace to interfere in the US election process. US authorities saw the move as reflecting a longstanding wish by Russia to destabilise the US-led liberal democratic order.[36] The interference was carried out via cyber operations targeting the two main Presidential candidates and use of social media to influence public opinion.[37] Russia was believed to have gained continued access to elements of several US state or local electoral boards.[38] The US intelligence community assessed that the interference was directly ordered by the Russian President aiming to support the election of Donald Trump.[39]

Consequently, the US government imposed new sanctions on Russia including the expelling of some diplomatic staff and the shutting down of a couple of Russian compounds in the US. Sanctions were also imposed against certain individuals and Russian entities in response to what the US government described as 'Significant Malicious Cyber-Enabled Activities'.[40] Following the US Congress approval of additional sanctions against Russia in July 2017, the Russian government also counter retaliated by forcing the US government to reduce the number of its employees in Russia by more than a half.[41]

In April 2022. Hackers targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shutdown electrical substations in Ukraine. Researchers believe the attack came from the same group with ties to the Russian GRU that targeted Ukraine's power grid in 2016, using an updated form of the same malware. Again, in April 2022: Hackers targeted Ukraine's National Post Office with a DDoS attack, days after releasing a new stamp honoring a Ukrainian border guard. The attack affected the agency's ability to run their online store.[42] Likewise, in April 2022. The U.S. Treasury Department's Office of Foreign Assets Control attributed the March 29 hack of Ronin Network to a North Korean hacking group and

[34] CHOE SANG-HUNOCT, 'North Korean Hackers Stole U.S.-South Korean Military Plans, Lawmaker Says, *The New York Times, October 10*, 2017, www.nytimes.com <Accessed 3/11/2017>.
[35] See (n 30).
[36] (n 10).
[37] Olivia Solon and Sabrina Siddiqui, 'Russia-Backed Facebook Posts 'Reached 126m Americans' during US Election', *The Guardian, 31st October*, 2017. https://www.theguardian.com › Technology › Facebook <Accessed 16/12/2017>
[38] (n 10).
[39] (n 10).
[40] Evan Perez and Daniella Diaz, 'White House Announces Retaliation against Russia: Sanctions, Ejecting Diplomats', *CNN, January 3*, 2017, edition.cnn.com/2016/12/29/.../russia-sanctions-announced-by-white-house/index.html. <Accessed 16/12/2017>.
[41] Zack Beauchamp, 'Russia Is Retaliating against New US Sanctions in a Big Way', *Vox, July 30*, 2017, https://www.vox.com/world/2017/7/30/.../putin-russia-755-diplomats-us-embassy <Accessed 16/12/2017>.
[42] CSIS | Center for Strategic and International Studies, *Significant Cyber Incidents | Strategic Technologies Program*, https://www.csis.org › progr https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents#main-content; Accessed 01/05/2024.

announced sanctions against the hackers. The group stole over $540 million in Ethereum and USDC.[43]

Other incidents include that in February 2023 where a pro-Russian hacking group claimed responsibility for DDoS attacks against NATO networks used to transmit sensitive data. The attack disrupted communications between NATO and airplanes providing earthquake aid to a Turkish airbase. The attack also took NATO's sites offline temporarily.[44] In the same February 2023, Polish officials reported a disinformation campaign targeting the Polish public. Targets received anti-Ukrainian refugee disinformation via email. Officials claimed these activities may be related to Russia-linked hackers.[45] Again, in February 2023, A North Korean hacking group conducted an espionage campaign between August and November 2022. Hackers targeted medical research, healthcare, defense, energy, chemical engineering and a research university, exfiltrating over 100MB of data from each victim while remaining undetected. The group is linked to the North Korean government.[46]

Though the year 2024 in just in its first quarter, these incidents are replete across the globe. Examples include the following: in March 2024: Russian hackers launched phishing attacks against German political parties. Hackers concealed ransomware in a fake dinner invitation from Germany's Christian Democratic Union to install a backdoor in their victim's computer.[47] In February 2024: Russian hackers launched an espionage campaign against the embassies of Georgia, Poland, Ukraine, and Iran beginning in 2023. Hackers exploited a bug in a webmail server to inject malware into servers at the embassies and collect information on European and Iranian political and military activities.[48] In December 2023: Israeli-linked hackers disrupted approximately 70% of gas stations in Iran. Hackers claimed the attack was in retaliation for aggressive actions by Iran and its proxies in the region. Pumps restored operation the next day, but payment issues continued for several days.[49]

These incidents represent not only the new trends in the use of cyberspace to infringe national frontiers and infrastructure, but also measures taken in response to some of these actions. How this relates to the discourse on the use of force in international law will depend on several factors. While some of these factors may be considered from the definition and nature of the prohibition on the use of force, others may come from a critical analysis of the objectives and essence of the prohibition and the cyber activities.

3.0 THE PROHIBITION ON THE USE OF FORCE

The use of force by states was once recognised as the exclusive preserve of states in the exercise of their sovereignty.[50] Consequently, the decision to use

[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Ibid.
[50] O'Connell, Mary Ellen. '*The Prohibition of the Use of Force*' In Research Handbook on International Conflict and Security Law. (Edward Elgar Publishing, 2013).

force was considered of no consequence to third states whose rights were not directly affected.[51] As all the outstanding efforts at regulating, if not proscribing war could not avert World War II, the UN Charter regime, building on previous efforts,[52] took novel and courageous steps to prohibit not only war, but the use or threat of force in international law.

The prohibition on the use force under article 2 (4) of the UN Charter popularly regarded as the cornerstone of the UN Charter is now generally accepted as a norm of customary international law having the status of *jus cogens*.[53] Hence, this prohibition represents a communal resolve by the international community of nations to reject all attempts not only at using force against other states, but also threatening it. Most importantly, the unanimous agreement by all nations to the insertion of the term "against the territorial integrity and political independence of any state, or in any other manner inconsistent with the UN Charter" is instructive.[54] These wordings, clearly buttress the spirit of the prohibition which is the protection of sovereignty, territorial integrity, and political independence of states. This is made clearer when considered together with the fundamental principles upon which the United Nations was established. These principles are plainly discernible from the preamble of the UN Charter with reference to the provisions of Articles 1and 2 generally.[55] The prohibition under Article 2 (4) was not coincidental; it was well planned and deliberated upon even before the end of World War II.[56] It was therefore intended to guarantee a comprehensive proscription subject only to the precise exemptions specified in the UN Charter.[57] These exceptions basically are confined to self-defence under Article 51 and the collective security measures under Chapter VII. In enunciating the norms of Article 2(4) however, it is necessary to be mindful of its domineering characteristic, and the need to adapt it to the varying realities of international needs. This is so because the prohibition against the use of force has metamorphosed into customary international law, and even the status of jus cogens.[58] This will ensure the preservation of its fundamental connotation and worth, without discarding the flexibility needed to preserve it as a living law.

4.0 SELF-DEFENCE

The prohibition against the use force notwithstanding, where the existence or survival of a state is threatened, it/they has/have the right to defend itself/themselves. Consequently, Article 51 of the UN Charter recognises the

---

[51] Edward Gordon, 'Article 2 (4) in Historical Context', *Yale Journal of International Law*, [1985], (10) (2) 271–78. 271.

[52] Some of these efforts include the League of Nations, The Kellogg-Briand Pact signed on August 27, 1928.

[53] (n 15): see also ICJ Reports, Armed Activities on the Territory of the Congo (DRC v Uganda) (Merits) (2005).; The Nicaragua Case, n 2.

[54] Mohammed Barakat, '*The Legality of the Use of Force against Iraq in 2003*' (City University London, 2007). 14.

[55] United Nations, '(n 11)'.

[56] M. Goodrich L and E Hambro, *Charter of the United Nations; Commentary and Documents*, (2nd ed, Stevens & Sons, 1949,). 6-7.

[57] Ian Brownlie, 'International Law and the Use of Force by States - Revisited', in *A Europaeum Lecture Delivered at the Graduate Institute of International Studies, Geneva, on February 1st*, 2001, 1–26.

[58] Helmersen, Sondre Torp. "The Prohibition of the Use of Force as Jus Cogens: Explaining Apparent Derogations.*'Netherlands International Law Review'* {2014} (vol. 61),(no. 2): 167-193.

inherent right of states to individual and collective self-defence. It follows that this right to self-defence may be triggered by any action that may impact negatively on a state's survival, not necessarily disastrous situations.[59] The position that states may have recourse to their own mechanisms to defend themselves has always been a factual position reflecting the peculiar characteristic of states as subjects of international law.[60] But then, the right to self-defence has only become relevant because of the prohibition on the use of force. This follows logically as there was no need for any right to self-defence when states could legally resort to using force at will.[61]

Not every use of force may justify self-defence as the concept has restrictions in the context of Article 51. Consequently, an "armed attack" is a *sine qua non* to trigger the right to self-defence. A state may therefore, not claim the right to use force in self-defence unless it can establish the occurrence of an armed attack against it. Where the force used cannot be said to amount to an "armed attack", the victim state may only resort to other options including the Security Council for possible action under Chapter IV.[62]

The term "armed attack" has been severally defined by authors and other authoritative interpretations such as that of the ICJ.[63] However, despite the assertion that there may be some form of agreement as to what constitutes an armed attack,[64] one cannot with certainty accept such a general conclusion.[65] It is true that certain uses of force are generally accepted as satisfying the definition of an "armed attack". Having said that, it is also imperative to consider if, and to what level contemporary developments have transformed customary margins of the right to self-defence especially in relation to what constitutes an armed attack.[66] The concept of an "armed attack" as enshrined in the UN Charter therefore, accepts of an evolutive interpretation as well as adjustment founded on post UN Charter custom.[67] The customary practices of states especially in relation to contemporary developments should be seen as illuminating the provisions of the UN Charter. In such a situation, the UN Charter lives on to regulate international relations and serve as a source of direction for international law.

The right of states to self-defence therefore becomes available the moment force is applied against them in violation of the prohibition under Article 2 (4).

---

[59] Yoram Dinstein, *War, Aggression and Self-Defence*, (Cambridge University Press, 2005, 4th ed). 175.

[60] Yoram Dinstein, 'International Law as a Primitive Legal System', *NYUJ Int'l L. & Pol*. [1986] (19) (1) 12.

[61] (n 15)1398. 1399.

[62] (n 15), 1401.

[63] See for instance, Ruys, Tom. 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice. (Cambridge University Press, 2010), Todd, Graham H. "Armed attack in cyberspace: deterring asymmetric warfare with an asymmetric definition. '*AFL Rev'* 64 {2009}: 65., Feder, Norman Menachem. "Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack." *NYUJ Int'l L. & Pol*. 19. (1986): 395. See also, the Nicaragua Case; (n 2),14. 103 paras 194-98.

[64] The Nicaragua Case; (n 2),14. 103 paras 195.

[65] Claus Kreß, 'Armed Attack' and Article 51 of the UN Charter. Evolutions in Customary Law and Practice', [2014] (83) (1) *Bybil*; 145–60, doi:10.1093/bybil/brt010.

[66] Tom Ruys, *"Armed Attack"and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press, 2010). 3.

[67] ibid.

To argue that there could be what amount to a violation of Article 2 (4) against a state, yet not triggering the right to self-defence because it does not amount to an "armed attack" would amount to creating unnecessary and unrealistic lacunae.[68] This is unrealistic because where states cannot resort to a legitimate remedy where their sovereignty has been violated; they may resort to illegitimate ones to defend themselves.

5.0 PROPORTIONALITY AND NECESSITY

Though the requirements of necessity and proportionality are not specifically mentioned under Article 51, it is generally settled that an action in self-defence need to be necessary and proportionate to the armed attack.[69] These two elements are well established under customary international law and apply to any use of force pursuant to Article 51 of the UN Charter.[70] Thus, any action in self-defence must clearly be necessary in the circumstances, and whatever means employed to exercise such a right must be done while considering the attack triggering the right to self-defence – it must be proportionate.[71] The principle of necessity here addresses the query as to whether an exact action is needed to accomplish a valid purpose of self-defence. Proportionality on the other hand addresses the question as to how far a measure may go in order to accomplish the stated purpose.[72]

A legitimate exercise of the right to self-defence must therefore, inevitably establish an armed attack; this in addition to the definite proof of which state was responsible.[73] An armed attack must have been deliberately planned and directed at the victim state. This eliminates cases of mistake and accident or unintended consequences as opposed to astute planning towards an eventual victim.[74] It is also necessary to establish that force was the only option because there existed no other means of addressing the problem. Hence, to use force in self-defence, it must be such that all peaceful efforts have either been exhausted or that they would be pointless.[75]

Proportionality on the other hand requires that actions taken in self-defence should not go too far and used as punishment. Thus, though it admits of some flexibility, it requires that while countering force with force, states should be reasonable.[76] This means that a state acting in self-defence must consider the severity of the original attack and the magnitudes of the armed response to the attack generally.[77] This is not implying that the weapons used must be the same or comparable to those used in the original attack. It means that the action in self-defence should be limited to fend off the attack and to eliminate the precise

[68] On this, (n 15), 1401-2.
[69] (n 2). 94.
[70] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports, (1996). 245.
[71] *Oil Platforms (Islamic Republic of Iran v United States of America)*, ICJ Reports 161 (2003). 1361
[72] (n 15), 1426.
[73] (n 51). 209.
[74] William H. IV Taft, 'Self-Defense and the Oil Platforms Decision', *Yale J. Int'l L*, [2004], (29), 295. 302.
[75] Oscar Schachter, 'The Right of States to Use Armed Force', *Mich. L. Rev*, [1984] (82) (1), 620–46. 1635.
[76] (n 51) 210.
[77] *Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America*, ICJ Reports (2003). 37, Para 76.

compulsion from which the attack arose.[78] It therefore, would preclude moves to achieve additional advantages under the guise of self-defence. But then, so long as the actions of a state realistically maintain the principal aim of fending off the initial attack, it is irrelevant that it might have concealed motives.[79]

6.0 CYBER-ATTACKS AND THE USE OF FORCE

Contemporary reality of the use of cyberspace for several activities that may not only violate a state's sovereignty but also cause physical, material, defensive or human loss necessitate the consideration of cyber-attacks as use of force. Cyber-attacks could occur either in war times as was the case during Russia's invasion of Georgia, or in peace time as the attack on Iran's nuclear weapons. In both situations, such attacks could be equally devastating. Consequently, some authors conclude that all cases of cyber-attacks as opposed to simple cyber-crimes amount to use of force in international law.[80] However, it is easier to classify cyber-attacks in war times as use of force because they might have been an integral part of a broad war strategy. When cyber-attacks take place in peaceful times, it becomes necessary to assess all the relevant facts before concluding on its effect on the use of force. Incidents of cyber-attacks on defence-related infrastructure are also easier seen as acts of war as opposed to civil or civilian infrastructure.

It is true that cyber-attacks or cyber-activities generally could not have been contemplated in 1945 when the UN Charter was drafted. It follows therefore, that their emergence as contemporary phenomena will lead to the kind of chaos being experienced especially over the last two decades. However, cyber-attacks, notwithstanding their uniqueness, are capable of fitting into the broad definition of "armed force" or "armed attack" as the case may be. Consequently, it is stating the obvious that an armed attack is not defined by the type of weapon used.[81] In principle therefore, an armed attack may be carried out by means other than kinetic weapons.[82]

However, just as is the case with kinetic weapons, an armed attack is defined with reference to the effect of the attack. This being the case, it follows that the primary consideration should be the effect of such an attack be it cyber or conventional; as stated above, it is not about the type of weapon used. But then, to qualify as an armed attack, the effect must be considerable and proximately damaging.[83] Whether cyber-attacks need to produce the same effect as kinetic or other conventional weapons is another issue. The logical argument is that the attack must produce comparable effect to that which qualifies conventional

---

[78] (n 15), 1426.
[79] (n 66).
[80] Stephenie Gosnell Handler, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare', *Stanford Journal of International Law* [2012] (48) (1); 209–37. 210: Jozef Valuch, Cyber Attacks, Information Attacks, and Postmodern Warfare, *Baltic Journal of Law & Politics* (2017) (10:1) 910:1: 63–89 http://www.degruyter.com/view/j/bjlp DOI: 10.1515/bjlp-2017-0003, 72: Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Colum. J. Transnat'l L.* (1999) (37) 885, 938.
[81] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, I.C.J. Reports (1996). 226, para 39.
[82] (n 58), 515.
[83] (n 15), 1419.

attacks as armed attack.[84] Comparable here is not necessarily identical; it is comparable once the effect on the victim state is felt in similar proportion. Consequently, the nature and worth of the object of that attack is the primary threshold to determine whether the effect amounts to an armed attack. Where a state's infrastructure is destroyed through cyber warfare in such a way as to prevent it from carrying out basic or vital functions of statecraft, that may amount to an armed attack. In contemporary societies which rely so much on technology and electricity for instance, cyber-attack on these basic facilities will certainly disorganise the society and lead to chaos. This is in addition to the financial and material effects this might have on the economy of such a state. One can only imagine the dimensions of losses and destructions that will result from total power failure or shut down of internet facilities in advanced societies.

Hence, when Estonia was attacked in 2007, it was easy to draw analogy in NATO by the poser: "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?"[85] As a result, NATO had to take the stance that "cyber-defence is part of collective-defence."[86] This statement means that the collective defence organisation considers a cyber-attack as use of force which may give rise to military action. This position will also apply with respect to the attack on Iranian nuclear plant. Clearly, the nature and sensitivity of the object of attack qualifies it as a military target without having to prove specific damage. Though Iran did not claim any such right to self-defence against the US which was responsible for the cyber-attack,[87] it doesn't change the fact that the cyber-attack amounted to an armed attack.

Thus, looking at the cyber-attack on Sony Pictures, though much damage was done, it certainly is not comparable to any use of conventional weapons. This is not ignoring the other side of the damage which is to the sovereignty and integrity of the US as a sovereign state having responsibility to protect its citizens and their property.[88] The cyber-attack would certainly result in loss of confidence by the citizens in the level of protection their country can provide. Such a dent on the confidence of citizens and the international embarrassment may however, not be comparable to an armed attack in terms of the effects. This perhaps explain why the US government in retaliating, did not claim any right to self-defence against North Korea. Rather, a proportionate response was all that was promised and feasibly delivered.[89]

However, the attack on North Korea allegedly by the US in response to the Sony Pictures attack has the elements of a cyber-attack that might amount to an armed attack. This can be seen from the fact that the entire country's internet

[84] (n 72).
[85] (n 11) 78.
[86] NATO, 'Press Conference by NATO Secretary General Anders Fogh Rasmussen Following the Meeting of the North Atlantic Council at the Level of Heads of State and Government during the NATO Wales Summit', *05 September*, 2014, https://www.nato.int/cps/ic/natohq/opinions_112871.htm%0A<Accessed 18/12/2017>.
[87] (n 31).
[88] Michael N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013). 26.
[89] (n 31).

service was shut down for days. Though it is not clear how much North Korea relies on the internet for commerce, security, and general administration, it can certainly be assumed that substantial damage was done. If anything, it means that the entire country was cut off from the rest of the world and could not carry out transactions be it commercial, healthcare, or security. This retaliatory action therefore brings to the fore the issue of proportionality of measures taken in self-defence. But then, the US never claimed that North Korea's action amounted to an armed attack against it; hence no claim to self-defence was made. At the best, what the US did might only amount to a countermeasure, reprisal, or retorsion.[90]

The cyber-attack on the South Korean defence website is an attack on military infrastructure which may, depending on the damage done easily qualify as an armed attack. According to reports, some classified security documents were stolen, including contingency war plans.[91] The fact that such a sensitive infrastructure was invaded gives rise to the possibility of highly sensitive information being accessed. However, access to such information without showing the damage such access has caused may not be sufficient to justify classification of such an action as an armed attack; this is necessary to justify military action. Unfortunately, the sensitivity of such an information and the possible embarrassment the hack might have caused South Korea meant that they could not admit to the exact damage caused.

The cyber-activities allegedly by Russia targeted at influencing the US elections may not easily fit into the definition of an armed attack for several reasons. For a start, the cyber-activities were carried out mainly on social media with the primary aim of influencing the opinion of voters in favour of a candidate.[92] For another thing, no material, physical, human, or any tangible damage can be identified from the Russian actions. Though attempting to influence the outcome of elections in another sovereign state in such a brazen way may amount to invading its sovereignty, it is difficult to equate it with an armed attack. It may not have amounted to anything new from the espionage and sabotage nations engage in against each other.[93] The most problematic aspect of the Russian cyber-activity was its gaining and maintaining access to the databases of several electoral institutions in the US including that of the major political parties.[94] Accessing the data bases of vital political and electoral institutions of another sovereign state is certainly an aggressive invasion of its sovereignty. However, the damage caused was not substantial from the US's own assessment;[95] it did not amount to an armed attack. The Russian cyber-

[90] For more on this, see Malcolm N Shaw, *International Law*, (8th ed. Cambridge University Press, 2017). 1178-9.
[91] (n 34).
[92] (n 10)."
[93] See S Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law', *Michigan Journal of International Law*; [2006] (27) (4) 1071–1130.
[94] (n 10).
[95] (n 80).

activities would however, amount to a violation of the principle of non-intervention in the domestic affairs of a state.[96]

But then, there is the other side of the argument; if the prohibition of the use of force is meant to protect the sovereignty and political independence of states, any hostile action aimed at undermining these precepts may fall under the prohibition. The addition of the qualification "against the territorial integrity and political independence of a state" was meant to reinforce the prohibition.[97] That being the case, any hostile action the objective of which is to invade that political independence will clearly qualify as a prohibited act.[98] Seen from this light, the Russian cyber-activities are actions targeting the political independence of the United States of America. This is so because the cyber activities were meant to have unprecedented influence on the US political system ultimately resulting in the emergence of a pro-Russian US president.

Moreover, the prohibition being against the territorial integrity of a state also calls for consideration of the cyber activities here including that of the US against North Korea and the cyber invasion of the Iranian nuclear reactor. The North Korean cyber-attack against the South Korean defence system can also be considered from this background just as the Russian cyber-activities. The territory of a state is ordinarily a clear and factual matter discernible from the physical frontiers of the state. However, when talking of cyber activities or the cyber space generally, it may not be so easily defined.[99] For one thing, the cyber space being virtual space requires a different definition of national frontiers. It may not be enough to say that there are no national frontiers on the cyber space; truth is that there are. Nations generally exercise control on what happens on the cyberspace within their jurisdiction. And that includes legislation and regulation of the space within their frontiers. Consequently, some states censor the contents and general information that reaches people within their jurisdiction through the cyber-space. Indeed, even cyber-based businesses must undergo the regulatory procedure of obtaining licenses to operate within the frontiers of states cyberspaces. In addition, while operating within national frontiers though on the internet, multi-national companies pay taxes to the governments of such states. This is a clear acknowledgement of the state's sovereign control over such a virtual space as part of their territory. This being the case, any invasion of this territory amounts to an invasion of the state's territory.[100] Since aggressive invasion of territory qualifies as use of force against that state, cyber-attacks though virtual, and even without resulting in physical damage, amounts to an aggressive invasion of territory.

---

[96] See United Nations, n 11 art. 2 (1) & (4); Kawser Ahmed, 'The Domestic Jurisdiction Clause in the United Nations Charter: A Historical View', *Singapore Yearbook of International Law*: [2006] (10)175–97.

[97] (n 46); 14-15.

[98] Pascal Brangetto, Tomáš Minárik, and Jan Stinissen, 'From Active Cyber Defence to Responsive Cyber Defence: A Way for States to Defend Themselves – Legal Implications', in Dr Petra Ochmannova (ed) *Legal Issues Related to Cyber*, (35th ed, Monte DeBoer, 2014), www.nato.int <Accessed 20/12/2017>. 20.

[99] For general discussion on this, see Heinegg Von and Wolff Heintschel., 'Legal Implications of Territorial Sovereignty in C. Czosseck, R. Ottis, and K. Ziolkowski ed. *Cyberspace', in Cyber Conflict (CYCON), 2012 4th International Conference*, (Tallinn: NATO CCD COE Publications, 2012), 1–13.

[100] (n 90); 20.

7.0 CAN CYBER-ATTACKS TRIGGER THE RIGHT TO SELF-DEFENCE?

Whether a cyber-attack can trigger the right of self-defence under Article 51 of the UN Charter depends on the question of what amounts to an "armed attack". Therefore, the definition of an armed attack in relation to the prohibition of the use of force under Article 2 (4) is pivotal here.[101] In as much as a cyber-attack may present the necessary features of an armed attack such as immediate destruction or invasion of territory, it may still not be an easy task to establish.[102] For one thing, the people responsible for the attack may not be easily ascertained with the degree of certainty required to establish an important legal right as this. For another thing, there is also the possibility of error in identifying the perpetrators or their allegiance. As seen in recent events, the attackers do a good job of hiding or even diverting their identity. As a result, it is possible to point at the wrong party and eventually attack such party. It is also a possibility that states may deliberately point at the party they want to be guilty and present concocted evidence to that effect. As seen from the experience of the US invasion of Iraq,[103] this is highly likely.

A potentially more difficult problem would be on how to attribute the activities of the perpetrators to a state. As seen from the contemporary cases examined, hackers generally develop intricate techniques to evade detection. In some cases, they create misleading traces to lead any attempt to find them astray. It is also necessary to consider the fact that to exercise the right to self-defence, it is necessary that the action be taken expeditiously.[104] For a legitimate exercise of the right to self-defence, it is also necessary to show that the attack is on-going.[105] In cyber-attacks, it takes time to track down the perpetrators, identify them, and relate their activities to a sovereign state. Within such time as it would take to establish all these evidences, the requirement for acting expeditiously and the need for the attack to be on-going might have lapsed. Moreover, the trend in terms of contemporary cyber warfare is for states to use private individuals as may be seen in the case of North Korea and the other cases discussed.[106] In such circumstances, establishing a clear relationship between the perpetrators, even where they are traced, and a sovereign state may be difficult. This is more so when the high threshold required to establish attribution is taken into consideration.[107] Assuming all these challenges are successfully overcome, it would still be difficult to establish the necessity for such an action in self-defence; so also, the type of action needed to be taken in such a way that it would be proportionate to the original attack.

---

[101] See The Nicaragua Case (Merits), (n 2) . 103 paras 195.

[102] Georg Nolte and A. Randelzhofer. "Article 51 in Bruno Simma and others (eds.), The Charter of the United Nations: A Commentary (vol. II.OUP 2012), 1420.

[103] Sarah Left, 'Iraq War 'Waged on False Intelligence', *The Guardian, 9 July*, 2004. https://www.theguardian.com › World › Iraq <accessed 20/12/2017>.

[104] Marco Roscini, 'World Wide Warfare - Jus Ad Bellum and the Use of Cyber Force', in Armin Von bogdandy and R Wolfrum (eds) *Max Planck Yearbook of United Nations Law*, (vol. 14, Koninklijke Brill N.V, 2010); 85–130. 96.

[105] *(n 69).1*61, Para 57.

[106] See for example, BBC NEWS, 'Cyber-Attack: US and UK Blame North Korea for WannaCry', *19 December*, 2017, www.bbc.com/news/world-us-canada-42407488 <accessed 20/12/2017>.

[107] (n 94); 1420.

8.0 Necessity and Proportionality of Self-Defence in Response to Cyber Attacks

An action in self-defence differs from counter-measures, revenge, or punishment because it is carried out to repel an on-going attack. This is not ruling out the possibility of states resorting to counter-measures in cases of cyber-attacks.[108] Self-defence therefore, requires that the action taken is necessary to fend off an attack and possibly to displace the source of the attack; it should also be proportionate.[109] With cyber-attacks therefore, what would be the appropriate action in self-defence? Would it be at the stage where the state being attacked develops technologies capable of fending off the attack and preventing it from having access to its facilities? Self-defence should literally be to fend off an attack, and only attack when it is necessary for such defence.[110] Moreover, if the attack had already ceased by the time the perpetrators are identified, can the victim state legitimately claim any right to self-defence? Can states use kinetic force in response to cyber warfare?

Clearly, it would be difficult to claim the right to use kinetic force in response to cyber-attacks especially that which does not result in damaging consequences comparable to military attacks.[111] One of the most realistic ways to exercise the right of self-defence against an on-going cyber-attack which would satisfy the requirement of necessity and proportionality is by applying responsive cyber measures; otherwise referred to as Responsive Cyber Defence (RCD).[112] This is the fortification of a selected Communications and Information System (CIS) against a continuing cyber-attack by using procedures directed against the CIS from which the cyber-attack was initiated, or against third-party CIS involved in the attack.[113] This way, the cyber-attack is repelled while it is on-going and the response is directed against the originator of the attack. It also satisfies the requirement of proportionality as the response is similar in character to the attack.

9.0 FINDINGS

Having gone through vast literature on cyber warfare and the use of force in international law, including the actions and statements of states, this paper finds:

That contemporary trends indicate rising incidents of the use of the cyber-space to carryout devastating attacks on national institutions which may have security, economic, or other similar ramifications.

That there is the high tendency of the cyberspace being used to carry out what may amount to an armed attack against other nations.

---

[108] (n 80). Rule 9.
[109] Christine Gray, *International Law and the Use of Force*, (3rd ed, Oxford University Press, 2008). 148.
[110] *Case Concerning Oil Platforms, (n 69)* 161. Para 143; *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* 1996. 226 para 141.
[111] Matthew Waxman, 'Cyber Attacks as Force under UN Charter Article 2(4)', *International Law Studies*; [2010] (87) (4) 43–57. 48.
[112] (n 90); 17.
[113] ibid.

That powerful nations have always considered these activities as attacks on their national security structure.

That nations have carried out retaliatory attacks on those they believe are responsible for acts of cyberwarfare against them.

That the prohibition against the use of force under article 2 (4) of the UN Charter and the corollary right to self defence may clearly accommodate acts of cyber warfare depending on the magnitude the attack and the proportionality of acts carried out in self defence.

10.0 RECOMMENDATIONS

Considering the findings of this research, it is recommended that:

Nations should desist from carrying out or abetting acts in the cyberspace that may jeopardize the security, economic, or national interests of other states as that may likely be interpreted as an act of cyber warfare by the affected state. This is necessary because once it is so interpreted, then the chances are that the affected state may see them as acts of cyberwarfare capable of activating its right to self defence.

That when so ever the opportunity presents itself, international tribunals and institutions should provide detailed rules on how to deal with the issue of cyberwarfare, and the necessary response thereto.

11.0 CONCLUSION

Contemporary events prove that Cyber-attacks and cyber-warfare at the international level are factual, easier, cheaper, and more convenient for states. Therefore, it must be confronted and properly regulated in International law as it cannot be wished away. Article 2 (4) of the UN Charter aims at protecting the sovereignty, political independence and territorial integrity of all states; this reflects the spirit of the UN Charter. It is therefore necessary to interpret article 2 (4) in line with contemporary realities reflecting the intended protection. The right to self-defence under Article 51 being an inherent one means that states can resort to it whenever their survival is threatened. Contemporary developments have transformed the customary margins of self-defence illuminating the UN Charter as a living document. Violations of Article 2 (4) by way of cyber-attacks should trigger the right to self-defence; to argue otherwise would lead to unnecessary lacunae. However, actions taken in self-defence in response to cyber-attacks should be necessary and proportionate. This is easier proved where such an attack occurred in times of war; otherwise, it must be assessed in line with the general rules on the use of force. Suffice it to say that the need for comparative effect to that of conventional use of force does not mean identical effect. Cyber-attacks, notwithstanding their novelty, can fit into the legal framework on the use of force in international law.