Cyberspace in a State of Flux: Regulating cyberspace through International Law

Maxron Holder*
DOI: 10.21827/GroJIL.9.2.266-280

Keywords:
PUBLIC INTERNATIONAL LAW, DOMESTIC LAW, CONVENTION ON CYBERCRIME, CYBER AGRESSION, CYBERSPACE

Abstract

Cyberspace continues to become increasingly integral to our way of life. It has brought with it many benefits but has recently become a domain used for misdeed, as was evident from the recent WannaCry ransomware, the Stuxnet virus issue, and the much-publicized US 2016 Election hacking. These incidents have caused the issue of cyberspace to be on the international agenda, but there is a lack of consensus among the various nations on how cyberspace should be regulated. The article analyzes the legal status of cyberspace by first embarking on a discussion on what is cyberspace, followed by a discussion on recent notable cyberattacks. It is against this backdrop that: (1) the legal status of cyberspace in domestic law is analyzed; (2) the application of the existing rules of international law to cyberspace are considered; (3) the problems with the Budapest Convention on Cybercrime are discussed; and (4) proposals for a new Convention on cybersecurity at the UN level in light of the Tallinn Manual, and the Budapest Convention of Cybercrime are made.

I. Introduction

Defined as 'the notional environment in which communication over computer networks occurs',[1] cyberspace has, in recent decades, become woven into the fabric of societies around the world,[2] becoming the most highly demanded service in contemporary times. It is nowadays considered a global norm, offering its users because of its open and global nature great advantages in political, economic, social and information domains. At the same time, however, cyberspace can be the source of new and unpredictable threats non-existent in other environments, thus necessitating the need for effective regulations and enforceable laws.

In this article, I critically analyse the current legal state of cyberspace and have advocated for a treaty to regulate cyberspace. The article embarks on a discussion on what is cyberspace, followed by a discussion on recent notable cyberattacks. It is against this backdrop that: (1) the legal status of cyberspace in domestic law is analyzed; (2) the application of the existing rules of international law to cyberspace are considered; (3) the problems with the Budapest Convention on Cybercrime are discussed; (4) and proposals for a new Convention on cybersecurity at the United Nations (UN) level in light of the Tallinn Manual, and the Budapest Convention of Cybercrime are made.

* LL. B(Hons.) UWI, LEC (Candidate) Hugh Wooding Law School, holdermaxron@gmail.com.

1 *Oxford Dictionary of English* (3rd edn, Oxford University Press 2010).

2 Barrie Sander, 'Cyber Insecurity and the Politics of International Law' (2017) 6(5) European Society of International Law Reflections 1, pg.1.

II. What is Cyberspace?

According to Clough, '[t]echnology brings you great gifts with one hand, and it stabs you in the back with the other'.[3] Cyberspace is often presented as a purely non-legal domain.[4] It is ubiquitous and borderless thus no definition embraces all of its possibilities. A comprehensive definition which aims to encompass its uniqueness is coined by Kuel. Kuel believes that cyberspace is a global domain within the information environment. Besides, Kuel argues that the 'distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information-communication via interdependent and interconnected networks using information-communication technologies'.[5] The definition contains a threefold layers division: (1) physical layer which consists of computers, cable, communications infrastructure; (2) a second layer which consists of software programs and logics; and (3) a third layer which consists of data packets and electronics,[6] showing that cyberspace, although a virtual domain is braced by physical objects which connect the irreducible part of cyberspace to the physical world and interaction, is independent of constraints whether space or time.

It is misconceived that cyberspace is the internet, but in reality, cyberspace goes far beyond the internet.[7] However, this does not mean that they are acquaintances, as the internet comprises the main component of cyberspace. The internet is one of the significant cyberspace channels[8] as internet network providers exchange their traffic at physical sites located across the globe by cables beneath the earth and oceans, making the man-made domain of cyberspace a reality. The internet operates on a communications protocol which breaks messages into small blocks, or packets, fired across a network through the fastest route available at a particular time to reach their final destination where the messages are then reassembled.[9] While the usefulness of the internet and cyberspace is universally acknowledged, its misuse in the form of cybercrimes and espionage cannot be ignored. Today, governments and private corporations conduct most of their functions and activities in cyberspace, and the increasing reliance on cyberspace for daily living is multiplying by the minute.[10] Thus, safety, protection, and resilience in the cyberworld are matters of prominence.

---

3 Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015) 3.

4 Nicholas Tsagourias, 'The legal status of Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Edgar Publishing 2015) 13.

5 DT Keul, 'From Cyberspace to Cyberpower: Defining the Problem' in Franklin D Kramer, Stuart H Starr and Larry K Wentz,*Cyberpower and National Security* (National Defense Press 2009) 28.

6 Lior Tobanksy, 'Basic concepts in cyber warfare' (2011) 3 Military and Strategic Affairs 75, 77-78.

7 Peter W Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press 2014) 3.

8 Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (1st edn, Springer International Publishing 2017) 3.

9 ibid

10 ibid.

III. The Spectre of Cyber Aggression, Recent Cyberattacks and the Call for International Regulation

The growing availability of internet access and decreasing access costs have resulted in essentially anonymous global access, which increasingly facilitates the availability, assembly and use of cyber weapons on a global scale.[11] Nowadays, hackers can steal money through online bank accounts, they can hack university networks, modern cars can now be hacked by intercepting their computer-controlled navigation systems and much more because the possibilities of cyberspace are endless.[12] Generally, cyberattacks are separated into three major categories: (1) automated malicious software delivered over the internet which utilizes a computer system to infect a computer system; (2) denial-of-service attacks which overwhelms a computer system until it cannot function properly; and (3) unauthorized remote intrusions into computer systems which involves accessing a computer system without permission.[13] Most attacks taking attention in the News today fall within one of these distinct categories, which sometimes overlap.[14]

A notable example of cyberattacks falling within a category was the Stuxnet virus used to disrupt Iran's nuclear facilities in 2010. The Stuxnet virus uncovered in 2010 was widely reported to have been developed by the United States (US) and Israeli intelligence. It penetrated the rogue nuclear program of Iran, taking control and sabotaging parts of its enrichment processes by speeding up its centrifuges. Up to 1,000 centrifuges out of 5,000 were eventually damaged by the virus, setting back the nuclear program.[15]

The surveillance activities of the US National Security Agency (NSA) alleged in the disclosures of Edward Snowden in 2013[16] is also of critical importance with regards to the right to privacy. BBC reported that the scandal broke in early June 2013 when the Guardian newspaper reported that the NSA was collecting the telephone records of tens of millions of Americans.[17] The paper published the secret court order directing telecommunications company Verizon to hand over all its telephone data to the NSA on an 'ongoing daily basis'.[18] That report was followed by revelations in both the Washington Post and Guardian that the NSA tapped directly into the servers of nine internet firms, including Facebook, Google, Microsoft, and Yahoo, to track online communication in a surveillance programme known as Prism.[19]

---

[11] William M Stahl, 'The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity' (2011) 40(1) Georgia Journal of International and Comparative Law 247, 254.

[12] Kittichaisaree (n 8) 265.

[13] Matthew J Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent' (2009) 201(1) Military Law Review 1, 14.

[14] ibid.

[15] Stuart Winer, '"Dutch mole" planted Stuxnet virus in Iran nuclear site on behalf of CIA, Mossad' (*Times of Israel*, 19 October 2019) <https://www.timesofisrael.com/dutch-mole-planted-infamous-stuxnet-virus-in-iran-nuclear-site> accessed 1 October 2019.

[16] Sander (n 2) 2.

[17] ibid.

[18] ibid.

[19] BBC, 'Edward Snowden: Leaks that exposed US spy programme' (*BBC News*, 17 January 2014) <https://www.bbc.com/news/world-us-canada-23123964> accessed 1 October 2019.

The WannaCry ransomware that attacked computers across the world in 2017 has been subject to much international conversation.[20] The WannaCry incident involved hackers exploiting malicious software stolen from the NSA. It executed damaging cyberattacks that hit dozens of countries worldwide. One website reported that it forced Britain's public health system to send patients away, froze computers at Russia's Interior Ministry, and wreaked havoc on tens of thousands of computers elsewhere. According to Sanger:

> [T]he attacks amounted to an audacious global blackmail attempt spread by the internet and underscored the vulnerabilities of the digital age. The malicious software, which was transmitted by email, locked British hospitals out of their computer systems and demanded ransom before users could be let back in — with a threat that data would be destroyed if the demands were not met.[21]

The Guardian reported that 'in October 2016, the United States accused Russia of hacking political organizations involved in the US elections and leaking pilfered information to influence the outcome'.[22] According to US intelligence officials, Russian hackers made repeated attempts before the 2016 elections to get into major US institutions, including the White House and the State Department. According to one news article online, the tactics were simple: send out volleys of phishing emails and hope that someone clicked.[23] One of those who did was John Podesta, the chairman of Hillary Clinton's campaign. A New York Times investigation revealed that a Podesta aide spotted the dodgy email and forwarded it to a technician. This allowed Moscow to access about 60,000 of Podesta's emails. The hackers also breached the Democratic National Committee (DNC). The emails were passed to the WikiLeaks website, which published them before the US election. The furor dominated the news bulletins and damaged presidential candidate Hilary Clinton's campaign. Security experts believe that two Kremlin-connected groups were behind the hacks: one from the FSB spy agency; the other from Russian military intelligence.[24] This unearths the interference of a government into the domestic affairs of another country and realistically, it is impossible to hold such a government accountable under the regular domestic provisions given the principle of sovereignty of nations which is of prominence in international law.[25]

In 2014, North Korea was held responsible for hacking Sony in an attempt to prevent the release of a film that was baleful to the North Korean leader Kim Jong Un.[26] In late November 2014, Sony Pictures Entertainment was hacked by a group calling itself the Guardians of Peace. The hackers, who are widely believed to be working in at least some capacity with North Korea,

---

[20] Nicole Perlroth and David E Sanger, 'Hackers Hit Dozens of Countries Exploiting Stolen NSA Tool' (*The New York Times*, 12 March 2017) <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html> accessed 20 October 2019.

[21] Perlroth and Sanger (n 20).

[22] Luke Harding ,'What we know about Russia's interference in the US election' (*The Guardian*, 16 December 2016) <https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election> accessed 14 October 2019.

[23] ibid.

[24] ibid.

[25] David Harris and Sandesh Sivakumaran, *Cases and Materials on International Law* (7thedn, Sweet & Maxwell 2015).

[26] Emily VanDerWerff and Timothy B Lee, 'The 2014 Sony hacks, explained' (*Vox,* 3 June 2015) <https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea> accessed 23 October 2019.

stole huge amounts of information off of Sony's network. They leaked the information to journalists, who wrote about demeaning things Sony employees had said to each other. Then the hackers, using one of their near daily communiqués via the website Pastebin, threatened to commit acts of terrorism against movie theaters, demanding that Sony cancel the planned release of 'The Interview', a comedy about two Americans who assassinate North Korean leader Kim Jong Un.[27]

The presence of hackers is growing by the day as more and more people are acquiring the relevant skills to access or manipulate computer systems to their advantage.[28] In 2014, Microsoft Taiwan Corp. unveiled research findings, including evidence that Asia has become the frontline battlefield for computer hackers and cyber attackers, striking 400 million computers around the world each year.[29] Every second, 12 computers are hacked or hit by computer viruses, the company said during a media briefing in which it gave details of seven global digital crime trends.[30] An October 2015 study by the Ponemon Institute determined that the average annual cost of cybercrime in the US is $15.42 million per the US company, which was an increase from $12.69 million only a year ago.[31] As the threat of cybersecurity continues to increase, and costs associated with that threat continue to rise, businesses are now forced to find ways to mitigate these damages.[32] Thus, the need for proper cyberspace regulations is of crucial importance now more than ever.

The above cyberactivities unearth a myriad of instances where there have been cyberattacks, but it is worth noting that they all span across international borders. There are few reported cases of cyberactivities within the domestic domain for which domestic laws may be conveniently applied. However, the source of these activities is usually unknown, and investigations carried out by domestic cyber professionals are sometimes inconclusive as skilled attackers can lead investigations into trails to which they desire.[33] The application of domestic laws in the above situations must be based on the international corporation, and with the growing reluctance of States to assist in international investigations in another State, these regulations would not reach their full potential.[34] Thus, the use of domestic statutory provisions, while of crucial importance in regulating internal cyberactivities is now under scrutiny to meet the new demands of cyberspace which have proven to be a burdensome chore.

---

27 VanDerWerff and Lee (n 27).

28 Scott J Shackelford and others, 'Toward a Global Cybersecurity Standard of Care: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices' (2015) 50(1) Texas International Law Journal 305, 308.

29 CNA, 'Asia has become frontline for computer hackers' (*The China Post*, 27 November 2014) <https://chinapost.nownews.com/20141127-64669> accessed 20 October 2019.

30 ibid.

31 Ponemon Institute, *2015 Cost of Cyber Crime Study: United States* (Ponemon Institute 2015). <https://www.ponemon.org/news-updates/blog/security/2015-cost-of-cyber-crime-study-united-states.html> accessed 12 January 2022.

32 Andrew Z R Smith, 'FTC Regulating Cybersecurity Post Wyndham: An International Common Law Comparison on the Impact of Regulation of Cybersecurity' (2017) 45(1) Georgia Journal of International & Comparative Law 377, 378.

33 ibid.

34 ibid.

IV. Can Cyberspace be Regulated Sufficiently Through Domestic Law?

Given the increasing dependence of the world on cyberspace, it was inevitable for legislators of various nations to enact criminal offence to address online behavior.[35] Thus, many countries have implemented cybersecurity legislations.[36] Still, challenges arose in regulating cyberspace at the domestic level. One of the most important challenges is the issue of jurisdiction over offenders who may be located anywhere in the world. Thus, both the internet and computer networks have deeply changed contemporary legal systems. As a network spanning the globe, cyberspace offers criminals multiple refuges that cannot easily be detected. Therefore, the problem with holding a perpetrator liable is finding them. Studies show that the most popular of cybercrimes occur across international boundaries, showing the insufficiency of domestic law to address transnational cybercrimes.[37] The rise of a global computer network is destroying the power of local legislatures to assert control over cyberspace. Cyberspace has no territorial based boundaries. Cyberspace is independent of physical location. Location in these jurisdictions remains vitally important. Thus, efforts to control the flow of information across physical boarders are likely to prove futile. Individual electrons can easily, and without any realistic prospect of detection, enter any foreign territory. Cyberspace has thrown the law into disarray by creating an entirely new phenomenon that needs to become subject to clear international law rules.

Moreover, technology has created new types of offences of the like that have never been seen before. Offences arising from the field of computer crimes now affects traditional rights, such as copyright and privacy. Technology has also obscured the traditional national boundaries as information on the internet tends to be omnipresent. Thus, it has challenged the very notion of law as enforced through palpable sanctions in the nation State. Hacking offers a good example; it can originate anywhere in the world, and it is not hindered despite prevailing criminal laws against its prohibition. This is the traditional way of regulating cyberspace which was through the narrow lenses of domestic law. However, cyberspace has now had an impact on a larger and worldwide scale. Thus, in many countries, cyberspace is at a crossroad and there is no direction for legal practitioners and scholars on this issue.

There is also no cooperation among States on the issue of cyberspace. Where cases arise that have a foreign source, there is a need for States to cooperate on these cross-border investigations for domestic legislation to work. Without the cooperation of other States, wrongdoers cannot be prosecuted thus, making the domestic law futile.

Another problem faced at the domestic level is a lack of infrastructure and professionals to carry out these cyber related investigations.[38] The lack of professional training in the field of technology by law enforcement officials has contributed significantly to the struggle towards cybersecurity nationally, giving the perpetrators the upper hand in the war against cyberattacks.[39] Thus, the provisions are disempowering as they are not met with the relevant enforcement capacity.

---

[35] Smith (n 32) 378.

[36] UK's Computer Misuse Act 1990; Australia's Criminal Code 1995, parts 10.7-10.8; Canada's Criminal Code, sections 148, 342, 402-403; United States' Computer Fraud and Abuse Act.

[37] Singer and Friedman (n 7) 69.

[38] Martha Finnemore and Duncan B Hollis, 'Constructing Norms for Global Cybersecurity' (2016) 110(3) The American Journal of International Law 425, 450.

[39] Finnemore and Holli (n 38) 450.

The foregoing has shown that many countries across the globe have a legislation to regulate cyberspace.[40] However, the traditional way of regulating cyberspace through the narrow lenses of domestic law can no longer survive alone. There is a need for a treaty to regulate cyberspace to complement these domestic laws. This would provide cooperation and support with regard to investigating and prosecuting wrongdoers.

V. Can Cyberspace Be Regulated Through Existing Rules of International Law

A. What is International Law and its Relevance to Cyberspace?

The definition formulated by Professor Shearer is that body of law which is composed for its greater part of the principles and rules of conduct which States feel bound to observe, and therefore, do commonly observe in their relations with each other.[41] To date, international lawyers have primarily engaged with issues of cybersecurity by examining the extent to which existing international legal frameworks already apply to cyberactivities.[42] This engagement reflects a clear preference amongst international lawyers and scholars for elevating rules of international law to manage contemporary problems in cyberspace. This posture has also been legitimised by States and international organizations, many of which have affirmed the application of existing international law rules to cyberactivities.[43] As activists for the application of existing rules of international law to cybersecurity, international lawyers are inescapably embroiled in the exercise of legal interpretation to fit this jigsaw puzzle into place.

A careful analysis is required to correctly understand how existing public international law applies to cyberspace. There seems to be an emerging consensus that cyberattacks have certain special characteristics that set them in some ways difficult for rules to apply existing rules of international law. However, there have been calls to still apply them. It is argued that this is more convenient, as Zimmermann correctly argued that the traditional ways of developing new rules of international law through multilateral agreements or the process of widespread State practice giving rise to customary international law can never catch up with new technological developments in cyberspace.[44] Thus, the existing rules of international law have to be applied, however imperfect they may be, to cyberspace.

The law governing international relations differs substantially from domestic law in that, unlike the legal system within a State, its application spans the globe. Thus, the ubiquity of cyberspace, which is not restricted by national borders, renders strictly single State regulation largely ineffective.[45] International law is essential to effectively ensure cybersecurity in the common interest of all States and without international law, cybersecurity cannot achieve its full potential.

---

40 Kittichaisaree (n 8) 326.

41 Ivan A Shearer, *Starke's International Law* (11th edn, Butterworths 1994) 3.

42 Sander (n 2).

43 Ingo Venzke, *How Interpretation Makes International Law: On Semantic Change and Normative Twists* (Oxford University Press 2012) 108.

44 Andreas Zimmermann, 'International Law and "Cyber Space"' (2014) 3(1) European Soc. International Law Reflections 1, 1.

45 Matthias C Kettemann, 'Ensuring Cybersecurity through International Law' (2017) 69(2) Revista Española de Derecho Internacional 281, 284.

While we can count a handful of international specialized conventions that may be applied to this space such as the Outer Space Treaty and the Budapest Convention on Cybercrime, there is currently no major international consensus. Furthermore, it is also difficult to identify any practice repeated over time that would count as customary law applicable to this space, nor has any specific case-law emerged in the area of cyberspace.

B. Applying the Principles of Criminal Jurisdiction Under International Law

Jurisdiction in the context of public international law refers to the legal competence of a State to make, apply, and enforce rules with regards to persons, property, and situations/events outside its territory, and the limits of that competence.[46] Professor Mann describes the term as a State's right under international law to regulate conduct in matters not exclusively of domestic concern.[47] Criminal jurisdiction is an important concept in international law as it concerns not just the extent of sovereign powers of States but limitations on those powers at the international level.[48] Sales concluded that the context of cybersecurity requires answers considering a range of the different questions. Following Sale's opinion, the questions refer to: (1) the person responsible for launching a particular attack; (2) court jurisdiction; (3) determination of the court's jurisdiction based on the attack or local attacker; and (4) the applicability of extradition treaties.[49] Concerning criminal jurisdiction in 1935, Harvard Law School conducted a study that resulted in a Draft Convention on 'Jurisdiction concerning Crime', which identified five traditional bases upon which a State can exercise criminal jurisdiction.[50] These are: (1) the nationality principle; (2) the territoriality principle; (3) the passive personality principle; (4) the universality principle; and (5) the protective principle.

Under the territoriality principle, given the fact that a State enjoys sovereign powers within its territory, a State may exercise jurisdiction for crimes that either started or ended in their respective borders. This principle is based on the assumption that the attacker is within the territory affected, but usually, in cyberspace, the attacker is sometimes millions of miles away in another country. Thus, this principle cannot be realistically applied to cyberspace.

Under the universality principle, States may exercise jurisdiction over international crimes committed anywhere in the world. The use of this principle has proven controversial as judges are reluctant to find jurisdiction based on the universality principle. Moreover, there is no established practice in which States exercise universal jurisdiction, properly so called and no case law exists in which pure universal jurisdiction has formed the basis of jurisdiction.[51] In its application to cyberspace, cybercrimes must be given the status of international crimes which would be the concern of the international community.[52] Still with the lack of consensus on the legal status of cyberspace in international law, this principle is of no use to the cyberworld.

---

46 Alina Kaczorowska-Ireland, *Public International Law* (5th edn, Routledge 2015) 356.

47 Frederick A Mann, *The Doctrine of Jurisdiction in International Law* (A W Sijthoff 1964) 9.

48 Kaczorowska-Ireland (n 46) 358.

49 Nathan A Sales, 'Regulating Cyber-Security' (2013) 107(4) Northwestern University Law Review 1503,1522.

50 Harvard Law School, 'Research in International Law' (1935) 29 The American Journal on International Law 1.

51 *Arrest Warrant of 11 April 2000 (the Democratic Republic of the Congo v Belgium)* [2002] ICJ Rep 3.

52 Sean Kanuck, 'Sovereign Discourse on Cyber Conflict under International Law' (2010) 88 Texas Law Review 1571.

The passive personality principle which was seen in the case of *Yunis v US*,[53] suggests that States may exercise jurisdiction to punish aliens for acts committed abroad against its nationals. This principle of jurisdiction is proven controversial where the national is not within the State of the jurisdiction of the State, and the extradition of persons to answer before domestic courts are usually discretionary or based on an extradition treaty which provides a multitude of exceptions.

The protective principle allows States to exercise jurisdiction where crime affects national security or other interests of a State. The following mentioned principle can have its application in limited circumstances in cyberspace, and it would have to reach the threshold of national interest. Thus, a cyberattack on government servers unearths such.

The nationality principle is worth mentioning. It involves the competence of a State to punish its nationals. This would also be limited in its application as it would seem to apply to instances where cyberattacks were carried out on the State by its own national. These situations are not popular as most attacks are carried out across international borders against persons who are not a national of the victim State.

C. Application of the Rules of Use of Force. Is a Cyberattack a Use of Force?

The prohibition on the threat of the use of force acquires a prominent place in international law. It was born out of customary international law, found a home under article 2(4) of the UN Charter and is now being held in abeyance after being awarded the status of *jus cogens*. Article 2(4) of the UN Charter provides that:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State or any other manner inconsistent with the purposes of the United Nations*.[54]

Dinstein opined that, 'the force prohibited is armed force. The general view is that the article does not preclude a State from taking unilateral economic or other measures not involving the threat or use of force, in retaliation for a breach of international law by another State.'[55] This suggests that the force prohibited is that of military force. The view is supported by Kaczorowska, who has the opinion that non-violent actions might be in breach of other provisions of the UN Charter.[56] However, today cyberspace is becoming a new field for tracking military operations, and as military experts have acknowledged, cyberspace is emerging as a new domain of war.[57] This is premised on the idea that cyberattacks could disable a government's installations and civilian infrastructure such as power grids, railways, oil pipelines, airlines, transportation systems, financial markets, etc. and thus threaten the life of a State.[58] As seen earlier, cases of cyberattacks have been increasing, and governments have been the target of cyberattacks, and in some cases, governments have been the main suspect in the attacks, for example, the US has been the target of several cyberattacks that are claimed to have been performed by China.

---

[53] *United States v. Yunis,* 681 F. Supp. 896, 1988 U.S. Dist. LEXIS 1857 (D.D.C. Feb. 12, 1988).
[54] Charter of the United Nations (adopted 24 October 1945) 1 UNTS XVI, art 2(4).
[55] Yoram Dinstein, *War, Aggression and Self-defence* (3rd edn, Cambridge University Press 2001) 81.
[56] Kaczorowska-Ireland (n 47) 689.
[57] Nazanin Baradaran and Homayoun Habibi, 'Cyber Warfare and Self-Defense from the Perspective of International Law' (2017) 10(4) Journal of Politics & Law 40, 40.
[58] Baradaran and Habibi (n 57) 40.

Another famous case is attacking in Estonia in April 2007, where for three weeks, the country was the target of cyberattacks, which caused the failure of official government websites, TV stations, banks, and so on.[59]

To define cyber warfare, and its relevance to the prohibition of the use of force under the UN Charter, the international community must somehow reach a consensus as to whether these activities are covered particularly by Article 2(4) and Article 51 that provides the right to self-defence. Article 2(4) of the Charter describes the original sentence on the use of force in international law but the question as to whether this extends its hands of gratitude to cyberspace is one that needs to be answered by the community of nations.

Article 51 of the UN Charter, which should be read alongside Article 2(4) provides 'nothing 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'.[60] There is not any definition of what constitutes an armed attack in the UN Charter. Thus, it is the submission of some academics that a cyberattack as the use of force should be defined by its intensity and effects and not based on tools used.[61] The merits for these arguments are found in the decision of International Court of Justice in the *Legality of the Threat or Use of Nuclear Weapons (Advisory opinion).*[62] In that regard, the court explained that an armed attack is the most severe form of using the force in terms of scale and its effect.[63] It is thereby inevitably argued by some that a cyberattack that causes fundamental destruction and the loss of human lives, or great material destruction could be considered as an armed attack, and requires the right of self-defence.[64] There is still no State practice to accept this form of attack to constitute an armed attack. States have not responded in self-defence under the UN Charter when they have been subject to a cyberattack. Thus, this unearths the reluctance of States to accept a cyberattack as a use of force.

D. The Principle of Non-Intervention?

The principle of non-intervention is the right of every sovereign State to conduct its affairs without outside interference.[65] Although the principle of non-intervention is found under Article 2(4) of the UN Charter, in the *Nicaragua case*, the International Court of Justice (ICJ) held that it is also part and parcel of customary international law.[66] Conceived in the Friendly Relations Declaration, the principle of non-intervention indicates that no State, for whatever reason, has the right to intervene in the internal or external affairs of another State.[67] The Declaration went on to state that armed intervention and all other forms of interference or attempted threats against the personality of the State or political, economic, and cultural elements of the State violate

---

59 ibid 41.

60 Charter of the United Nations (n 54) art 51.

61 Duncan B Hollis, 'Why States Need an International Law for Information Operations' (2007) 11(4) Lewis & Clark Law Review 1023, 1041.

62 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226.

63 ibid [262].

64 Baradaran and Habibi (n 57) 42.

65 *Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 [73].

66 ibid.

67 UNGA, 'Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations' (24 October 1970) UN Doc A/RES/2625.

international law. The Declaration also notes that no State may use or encourage the use of economic, political or any other type of measures to coerce another State, and that no State shall inter alia organise, assist, finance, or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State or interfere in civil strife in another State. While the formulation is somewhat ambiguous, the core meaning of an intervention is clear. It seems to be precise to a cyberattack, especially where it is aimed towards a government system by another government as all States should enjoy the right to non-intervention, and a State sponsored cyber operation is contrary to this principle. This principle has thus far provided a standard for future cyberspace regulation, but the sole fault in this application to cyberspace is its failure to regulate the actions of non-State actors.

VI. The Budapest Convention on Cybercrime: Why has it not Achieved Universality?

According to the International Governance Framework for Cybersecurity Website, to date, the only effort to develop a unitary procedural approach to cybercrime is the Budapest Convention on Cybercrime developed by the Council of Europe. It aspires to create a single set of cyber laws and procedures internationally to ensure that there is no safe harbor for cybercriminals.[68] The object and purpose of the treaty is to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It also contains a series of powers and procedures such as the search of computer networks and lawful interception.[69]

The Budapest Convention has been unsuccessful in achieving universality. As of July 2021, 66 States have ratified the convention, while a further two States had signed the convention but not ratified it.[70] Since it entered into force, countries like Brazil and India have declined to adopt the Convention on the grounds that they did not participate in its drafting.[71] Russia opposes the Convention, stating that adoption would violate Russian sovereignty, and has usually refused to cooperate in law enforcement investigations relating to cybercrime.[72] The absence of these States appears to be a deterrent for more signatories. States may have taken the view that without these cyber giants, the treaty is pointless. This is understandable as to regulate cyberspace there is a need for universality, meaning consensus at the international level.

Another deterrent appears to be signatory and ratification procedures. While the Council of Europe provides regulations for the accession of non-Member States to the Budapest Convention, the procedure for such includes a requirement for non-Member States to make a written request for accession, and scrutiny by Council experts to determine the compatibility of the domestic laws of the State in question with the standards of the Council of Europe. Moreover,

---

[68] Paul Rosenzweig, 'The International Governance Framework for Cybersecurity' (2012) 37(2) Canada-United States Law Journal 405, 419.

[69] Budapest Convention on Cybercrime (Opening of the treaty 23 November 2001, entry into force 1 July 2004) E.T.S 185.

[70] Council of Europe, 'Chart of signatures and ratifications of Treaty 185' <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185> accessed 11 July 2021.

[71] Jonathan Clough, 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation' (2014) 40(3) Monash University Law Review 698, 711.

[72] ibid.

non-Member States would have to finance their participation in the Convention. Thus, these have acted as further deterrents especially for States outside the Council of Europe.

III. Proposals for Regulating Cyberspace

A. Why a Treaty?

The most fundamental benefit of an international treaty regulating cyberspace is to provide certainty. This would enable States to know the nature of their international legal obligations with certainty. Currently under international law, States are unaware of what constitutes a cyberattack, and what are their obligations if such is instituted by another State or even non-State actors.

A treaty would also allow States to negotiate terms that they are going to be bound by. This would encourage compliance, and those States which sign and ratify the treaty will show that they are willing to be bound by the provisions within.

B. Can the Tallin Manuals be Used as a Guide?

With growing cyberactivity, the risk to States individually and to the international community as a whole, both States and multinational organizations are on the quest to seek solutions. Thus, the North Atlantic Treaty Organization (NATO) has engaged its Cooperative Cyber Defense Center of Excellence (CCD COE) to help facilitate the original Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0)[73] and the newly released Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[74] There was no significant change between the two, but a few points added for clarification. Some useful provisions for a Treaty on Cyberspace was extracted below:

> *A State may exercise territorial jurisdiction over: (a) cyberinfrastructure and persons engaged in cyber activities on its territory; (b) cyberactivities originating in, or completed on its territory, or (c) cyber activities having a substantial effect in its territory.*[75]

This rule (Rule 9) is premised on the basis for a State to exercise the jurisdiction given the physical or legal presence of a person or object. This unearths that a person will be subject to the laws of the territory on which the person is found.

> *A State may exercise extraterritorial prescriptive jurisdiction concerning cyber activities:*
> (a) *conducted by its nationals;*
> (b) *committed on board vessels and aircraft possessing its nationality;*

---

[73] Michael N Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge University Press 2012).

[74] Michael N Schmitt, *Tallinn Manual 2.0 On the International Law Applicable To Cyber Operations* (2nd edn, Cambridge University Press 2017) [Hereinafter Tallinn Manual 2.0].

[75] Schmitt (n 73) rule 9.

(c) *conducted by foreign nationals and designed to undermine essential State interests seriously;*
(d) *conducted by foreign nationals against its nationals, with certain limitations; or*
(e) *that constitute crimes under international law subject to the universality principle*.[76]

This rule (Rule 10) goes beyond that which is provided in Rule 9. It addresses the scope of a State's prescriptive jurisdiction regarding them outside its territory.

> *A State may only exercise extraterritorial enforcement jurisdiction concerning persons, objects, and cyber activities based on (a) a specific allocation of authority under international law; or (b) valid consent by a foreign government to exercise jurisdiction on its territory*.[77]

> *Although as a general matter, States are not obliged to cooperate in the investigation and prosecution of cybercrime, such cooperation may be required by the terms of an applicable treaty or other international law obligation*.[78]

> *A State bears international responsibility for a cyber-related act that is attributable to the State. and that constitutes a breach of an international legal obligation*.[79]

States bear 'responsibility' for their internationally wrongful acts according to the law of State responsibility as was discussed earlier.

> *Cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State*.[80]

> *Cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in or under its direction or control, or (b) the State acknowledges and adopts the operations as its own.*[81]

> *Cyber operations executed in the context of armed conflict are subject to the law of armed conflict*.[82]

> *Cyber operations may amount to war crimes and thus give rise to individual criminal responsibility under international law.*[83]

The Tallinn Manual can be considered as soft law; thus, it is not legally binding. However, many of its provisions should be considered when drafting the prospective treaty. Its provisions relating to the exercise of jurisdiction, whether territorial or prescriptive, should be the basis of exercising jurisdiction under such a treaty. Its regulations on non-State actors should also be of importance,

---

[76] Schmitt (n 73) rule 10.
[77] ibid rule 12.
[78] ibid rule 13.
[79] ibid rule 14.
[80] ibid rule 15.
[81] ibid rule 17.
[82] ibid rule 80.
[83] ibid rule 84.

especially with regards to State responsibility. There should also be provisions in such a treaty that a State will undertake all necessary measures to ensure no cyberactivities occur within its territory aimed at causing disturbances in another. What must also be of importance for drafting a cyberspace treaty which was excluded from the Tallinn Manual was a clause providing that all parties must undertake to assist other parties in the investigation of cybercrimes, which have a transnational element. It is only through this cooperation that domestic legislation on cyberspace can achieve their full potential.

C. How Useful is the Budapest Convention on Cybercrime?

The Budapest Convention has provided a number of measures for the regulation of cyberspace. It places positive obligations on State parties. It places an obligation on State parties to adopt legislation and other measures necessary to establish as criminal offences under domestic law in a number of categories. These included offences against confidentiality, integrity and availability of computer data and systems, computer related offences, content related offences, offences related to infringements of copyright and related rights, ancillary liability, sanctions, the search and seizure of stored computer data, real time collection of data. These positive obligations are essential for a treaty regulating cyberspace. It requires States to enact a legislation to criminalise computer misuse offences.[84]

The Convention also includes a provision granting a State party jurisdiction over offences committed within the State's territory. This allows a State to assert jurisdiction in computer crimes involving a computer system within its territory even if the perpetrator committed the offence from outside of the State. The Convention grants a State jurisdiction over its citizens who commit an offence outside of the state.[85]

The Convention makes further provisions for international cooperation and mutual assistance in criminal matters for the purposes of investigation or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic. It makes further provisions for the extradition between parties for criminal offences within the meaning of the treaty.[86]

The forgoing provisions are necessary as it affords enforceable cooperation between the host and the victim State. This would complement domestic laws in making them enforceable.

VII. Conclusion

Although cyberspace has become woven into the fabric of modern society, its regulation remains in a state of flux. While there exist some domestic legislation regulating cyberspace, recent notable cyberattacks have questioned the effectiveness of these pieces of legislation, and the existing rules of international law remain unclear in their application to cyberspace. The problems associated with the Council of Europe's Budapest Convention on Cybercrimes have impeded it from achieving international support. Thus, there is a need for discussions and negotiations at the UN level for clear rules, and provisions for cooperation in cybercrime investigations and proceedings. This interest is one not just of national concern but also of

---

84 Budapest Convention on Cybercrime (n 69) section 1 arts 2-6.
85 ibid section 3 art 22.
86 ibid section 3 arts 23-35.

international concern. Thus, it is best advanced by pursuing and collaborating partnerships, and a multilateral approach. In order to regulate cyberspace sufficiently, States must be willing to have open discussions about the threats of cybersecurity and the development of appropriate rules for its regulation. It must have universal application and consensus with all States making substantial contributions to the discussion.

*