6-2023

Cyberoperations and sovereignty in international law

Joel Wei Xuan FUN
Singapore Management University, joel.fun.2017@law.smu.edu.sg

CYBEROPERATIONS AND SOVEREIGNTY IN INTERNATIONAL LAW

The cyberspace is sometimes seen as having no jurisdictional boundaries, given that no single state controls the entirety of the cyberspace. At the same time, given how pervasive the cyberspace has become today, many important interests of states now lie in the domain of cyberspace. This uneasy tension has led to many questions involving the intersectionality between the state's sovereignty over its territory and the cyberspace, which is exacerbated when states use the cyberspace to conduct their myriad operations. This paper seeks to delineate permissible and impermissible cyberoperations and argues that the present international law on sovereignty is sufficiently robust for such delineations.

Joel **FUN** Wei Xuan[*]
Class of 2022 (LLB, BBM), SMU Yong Pung How School of Law

I. Introduction

1 In our globalised and interdependent age, the cyberspace has become an essential part of the smooth functioning of daily life both at the individual[1] and governmental levels. However, despite such economic interdependence and the ease of spread of ideas through the cyberspace, it is unfortunate that a system of capitalist peace has yet to take root,[2] evidenced by ongoing conflicts around the world,[3] including the recent Russo-Ukrainian conflict. While large-scale kinetic conflicts and conflict-related battle deaths have decreased significantly since

[*] This article is written in the author's personal capacity, and the opinions expressed in this article are entirely the author's own views.

[1] See *e.g.*, Slavomír Gálik & Sabína Gáliková Tolnaiová, "Cyberspace as a New Existential Dimension of Man", in *Cyberspace* (Evon Abu-Taieh, Abdelkrim El Mouatasim & Issam H. Al Hadid eds) (Intech Open, 2020).

[2] For an explanation and assessment of the capitalist peace theory, see *e.g.*, Erik Gartzke, "The Capitalist Peace" (2007) 51(1) American Journal of Political Science 166; Patrick J. McDonald, *The Invisible Hand of Peace: Capitalism, the War Machine, and International Relations Theory* (Cambridge University Press, 2012); Seung-Whan Choi, "Re-Evaluating Capitalist and Democratic Peace Models" (2011) 55 International Studies Quarterly 759.

[3] See Council on Foreign Relations, "Global Conflict Tracker" <https://www.cfr.org/global-conflict-tracker>. The Council for Foreign Relations helpfully maps out conflicts around the world but is assessed with respect to the potential impact on the US's interests.

World War II,[4] other smaller-scale conflicts which make use of means such as cyberoperations have become increasingly commonplace.[5]

2 Such operations appear to emanate from various sources; while some operations may be carried out by non-state affiliated cyber-vigilantes, others may be sponsored or supported by the state in some shape or form. An example of the latter is the hacking of Sony prior to the release of the film "The Interview" in 2014, which depicted the death of leader Kim Jong Un,[6] and was suspected of having been funded by North Korea.[7] Another example is the Stuxnet attack, which was targeted at causing damage to Iran's nuclear program.[8] But apart from these prominent examples, cyberoperations occur on a frequent basis,[9] which necessitates the formulation of rules to govern and regulate them.

3 On the international plane, international law serves as an important normative framework for states to assess the conduct of such acts. In particular, this paper will focus on the international law rules relating to state sovereignty to assess the legality of cyberoperations and seek to highlight the various controversies that lie in this nascent area of the law. The intersection between sovereignty and cyberoperations is a troubled one, not least because our present conception of state sovereignty is of considerable heritage,[10] but yet is expected to tackle

---

4 Max Roser, Joe Hasell, Basian Herre & Bobbie Macdonald, "War and Peace" <https://ourworldindata.org/war-and-peace>; see also, Steven Pinker, *The Better Angels of Our Nature: Why Violence has Declined* (Penguin, 2011).

5 See *e.g.*, United Nations Security Council, "'Explosive' Growth of Digital Technologies Creating New Potential for Conflict, Disarmament Chief Tells Security Council in First-Ever Debate on Cyberthreats" (2021) UN Doc SC/14563; Cyber Investigations, Forensics and Response, "Triple digit increase in cyberattacks: What next?" <https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks>.

6 "Sony Pictures Computer System Hacked in Online Attack" (2014) *BBC News* <https://www.bbc.com/news/technology-30189029>; "Whodunnit? The Mystery of the Sony Pictures Hack" (2014) *BBC News* <https://www.bbc.com/news/technology-30530361>.

7 Federal Bureau of Investigation, "Update on Sony Investigation" (2014) <https://www.fbi.gov/news/press-releases/press-releases/update-on-sony-investigation>.

8 See generally, James P Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War" (2011) 53(1) Global Politics and Strategy 23.

9 See *e.g.*, Centre for Strategic and International Studies, "Significant Cyber Incidents" <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>; Council on Foreign Relations, "Cyber Operations Tracker" <https://www.cfr.org/cyber-operations/>, both of which provide frequent updates on significant cyber incidents.

10 See Part III(A) of this article.

nascent real-world problems. This is compounded by the oft-slow evolution and development of international law,[11] which makes it an unwieldy tool in dealing with fast-evolving international problems in the cyberspace. This paper will then argue that this seeming misfit between these two domains is not as apparent as it seems, as sovereignty and sovereignty-related norms are sufficiently precise at present to delineate the line between permissible and impermissible cyberoperations.

II. Cyberoperations: state-sponsored or cyber-vigilantism?

4 The first important question that one must ask is how a state can be made liable for cyberoperations that have been conducted. Since states form the primary subjects of international law,[12] attribution of individuals' actions to the state is necessary to find the state responsible for the actions committed by the individual. Such rules "establish that there is an act of the State for the purposes of responsibility",[13] and such responsibility is the "necessary corollary of law".[14] These customary rules are codified in the International Law Commission's *Draft Articles on State Responsibility* ("***ARSIWA***").[15]

5 The more "direct" approach would be in attributing the acts to the state, and subsequently making out a breach of an international obligation by the commission of the aforementioned acts. As provided for in Article 2 of the *ARSIWA*, an internationally wrongful act is made out where an action or omission is attributable to the state under international law and constitutes a breach of an international obligation of the state. In this regard, the customary rules of attribution as reflected in the *ARSIWA* would provide us with a good starting point to determine whether the actions can be attributed to the state. These acts would

---

11 See *e.g.*, Keith Suter, "The Successes and Limitations of International Law and the International Court of Justice" (2004) 20(4) Medicine, Conflict and Survival 344 at 345.

12 James Crawford, "The System of International Responsibility" in *The Law of International Responsibility* (James Crawford, Alain Pellet, Simon Olleson & Kate Parlett eds) (Oxford University Press, 2010) at p 17.

13 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10 at 39.

14 Alain Pellet, "The Definition of Responsibility in International Law" in *The Law of International Responsibility* (James Crawford, Alain Pellet, Simon Olleson & Kate Parlett eds) (Oxford University Press, 2010) at p 3, citing C de Visscher, *La responsabilité des États* (Leiden, Bibliotheca Visseriana, 1924) at p 90.

15 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10.

include: (1) acts done by a state organ,[16] or persons exercising elements of governmental authority;[17] (2) acts of persons that are acting under the instructions of, or the direction or control of that state;[18] and (3) acts that are acknowledged and adopted by a state as its own.[19]

6 While it is perhaps inappropriate to delve into too much detail here on how such rules of attribution work, it suffices to say that these rules are flexible enough to accommodate actors who are not formally related to the state. For example, the International Court of Justice in its *Bosnian Genocide*[20] and *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*[21] decisions attributed the acts of entities that were under the effective control of the state, to the state.[22] The subsequent adoption and acknowledgement of the acts of a group of students by the state were also sufficient to attribute their acts to the state in the *Tehran Hostages* decision.[23]

7 However, when it comes to the attribution of acts to a state in the cyberspace, there are important questions of evidence that would invariably fall upon a judicial body seeking to attribute the acts of an actor to that of the state. This is because of the intentional obfuscation of these actions by the responsible individuals, causing difficulties in identifying the machines or IP addresses responsible for the hack. It has been pointed out that "[e]ven extensive efforts do not always produce

---

16 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10, Article 4.

17 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10, Article 5.

18 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10, Article 8.

19 International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries" (2001) UN Doc A/56/10, Article 11. For a list of cases that have engaged the foregoing rules, see generally, the United Nations Legislative Series, "Materials on the Responsibility of States for Internationally Wrongful Acts" (2012) ST/LEG/SER.B/25.

20 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (2007) ICJ Rep 43.

21 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14.

22 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [105]–[115].

23 *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)* (1980) ICJ Rep 3 at [74].

unequivocal proof".[24] Even if a state is able to obtain proof of such information, they may not always want to reveal such evidence since it may provide indications of their cyber-capabilities, or reveal vulnerabilities which may be exploited by malicious actors to perpetrate further operations.[25]

8 Furthermore, even if the acts in question are properly considered as those of a private individual and not attributable to the state, this does not immediately end the inquiry of whether the state has violated international law. The "indirect" approach to finding a state responsible for cyberoperations may be to invoke some obligation of due diligence against the state from which the cyberoperations emanated.[26]

9 On one view, due diligence is a standard by which the acts of a private actor can be attributed to the state.[27] However, such a view has yet to be adopted and can at best be taken to represent *de lege ferenda* (*i.e.*, what the law ought to be or may in the future be). *Lex lata* (*i.e.*, present law) is clear that due diligence does not exist as a rule of attribution, but instead as a primary rule. An obligation of due diligence is special in that it "establishes a link between primary norms and secondary rules of state responsibility and bridges the gap between the two sets of rules… trigger[ing] state responsibility, where otherwise non-attributable acts of non-state actors would lead to a legal vacuum".[28] Thus, it is an important means to find a state responsible for the actions of individuals without attributing their acts under the aforementioned rules on attribution.

---

[24] William Banks, "Cyber Attribution and State Responsibility" (2021) 97 International Law Studies 1039 at 1046; see also, Thomas Rid & Ben Buchanan "Attributing Cyber Attacks" (2014) 38 Journal of Strategic Studies 4.

[25] François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) at p 108.

[26] See generally, Antonio Coco & Talita de Souza Dias, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law" (2021) 32(3) European Journal of International Law 771.

[27] Luke Chircop, "A Due Diligence Standard of Attribution in Cyberspace" 67(3) International and Comparative Law Quarterly 643.

[28] Elif Askin, "Due Diligence Obligation in Times of Crisis: A Reflection by the Example of International Arms Transfers" (2017) *EJIL:Talk!* <https://www.ejiltalk.org/due-diligence-obligation-in-times-of-crisis-a-reflection-by-the-example-of-international-arms-transfers/>. Secondary rules refer to the rules which determine the legal consequences of the failure to fulfil obligations established by the primary rules. Primary norms instead refer to the norms, whose breach can be a source of responsibility: see generally, Eric David, "Primary and Secondary Rules" in *The Law of International Responsibility* (James Crawford, Alain Pellet, Simon Olleson & Kate Parlett eds) (Oxford University Press, 2010) at p 27.

10 While prevalent in the context of environmental damage,[29] such an obligation of due diligence can apply more generally as seen in the *Corfu Channel* decision, the first contentious case heard by the International Court of Justice.[30] There, the court was faced with the question of whether Albania was responsible for mines laid in the Corfu Channel which damaged English naval ships passing through it. While the court found that it could not be proven that Albania had laid the mines, with "no evidence in support" of this contention,[31] nor was there any collusion found with Yugoslavia to mine the waters,[32] it nonetheless found that Albania had violated the duty of due diligence. In reaching this conclusion, the court held that states are "not to allow knowingly its territory to be used for acts contrary to the rights of other States".[33]

11 However, the duty of due diligence is ultimately contextual in nature[34] and much depends on whether there is such a customary duty that exists in the cyberspace. As observed by Ponta, there are still major doubts by states as to whether there is any due diligence obligation that applies to the cyberspace, evidenced by the non-mandatory and vague language used by states when discussing due diligence in cyberspace in the 2015 UN Group of Governmental Experts ("**UNGGE**") report.[35] Thus, some have argued that in order to make out a customary rule of due diligence, states should encourage other states to accept cyber due

---

29 See *e.g.*, *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* and *Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)* (2015) ICJ Rep 665 at [104], citing *Pulp Mills on the River Uruguay (Argentina v. Uruguay)* (2010) ICJ Rep 14. See also, Rumiana Yotova "The Principles of Due Diligence and Prevention in International Environmental Law" (2016) 75(3) Cambridge Law Journal 445.

30 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4.

31 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4 at 16.

32 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4 at 17.

33 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4 at 22.

34 Neil McDonald, "The Role of Due Diligence in International Law" (2019) 68(4) International and Comparative Law Quarterly 1041 at 1054.

35 Adina Ponta, "Security and Human Rights Challenges of Cyber Due Diligence" (2020) Harvard International Law Journal Online <https://harvardilj.org/2020/06/security-and-human-rights-challenges-of-cyber-due-diligence/>. For the 2015 UNGGE Report, see UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015) UN Doc A/70/174.

diligence as a customary rule, by affording the rule *lex lata* status, and punishing states that violate these requirements.[36]

12 However, it is suggested that such an approach is unnecessary. Ultimately, it must be noted that the central enquiry is whether the due diligence obligation, which is a customary rule that applies generally, can extend to the cyberspace. Instead of having to inductively make out the *opinio juris* and state practice to constitute customary international law,[37] the more appropriate methodological approach may be to: (1) establish the underlying rule (*i.e.*, due diligence is a rule generally); and subsequently (2) see if the conclusion (*i.e.*, due diligence applies in the context of cyberspace) is unsupported by state practice and doctrine. This approach was provided by Judge Jessup in his separate opinion in *Barcelona Traction*,[38] and is a practical way to determine if a customary rule applies in a particular context, since "no survey of State practice can, strictly speaking, be comprehensive and the practice of a single State may vary from time to time".[39] Adopting this approach, it is difficult to see how the 2015 UNGGE report, which only hints at the conclusion that states *may* not endorse such a position,[40] can displace the general rule in *Corfu Channel*. Further, as Coco and Dias similarly observe, the disagreements by a limited number of states such as Argentina and Israel stand in contrast to many other states such as Chile, the Czech Republic, Denmark, the Dominican Republic, Ecuador, Estonia, Finland, France, Guatemala, Guyana, Iceland, Japan, Norway, Peru, the Republic of Korea, Sweden, and The Netherlands, which have started speaking up in support of the existence of due diligence obligations in the cyberspace.[41]

---

36 Olivia Hankinson, "Due Diligence and the Gray Zones of International Cyberspace Laws" (2017) Michigan Journal of International Law Online <http://www.mjilonline.org/due-diligence-and-the-gray-zones-of-international-cyberspace-laws/>.

37 For the requirement of state practice and *opinio juris* and what may amount to these requirements, see International Law Commission, *Draft Conclusions on Identification of Customary International Law, with Commentaries* (2018) UN Doc A/73/10.

38 *Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)* (1970) ICJ Rep 3.

39 *Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)* (1970) ICJ Rep 3 at [60] (Separate Opinion, Judge Jessup).

40 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 31.

41 Talita Dias & Antonio Coco, "Cyber Due Diligence in International Law" (2022) at p 28 <https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligenceininternationallawpdf.pdf>.

III. State sovereignty in cyberoperations

A. What is sovereignty?

13 State sovereignty has been deeply contested and an ever-changing concept in legal, political, and historical terms.[42] Broadly, however, we can say that sovereignty refers to the supreme authority within a state to govern its own territory, and forms one of the fundamental pillars of the modern system of international law.[43] As put forth in the *Island of Palmas* decision by the Permanent Court of Arbitration, "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[44] There are two key dimensions to sovereignty. Internal sovereignty broadly refers to the state's ultimate authority and competence over all people and all things within its territory, implicating principles such as non-intervention; on the other hand, external sovereignty refers to the state's relations to other states, implicating principles such as state immunity.[45]

14 Many have traced the consolidation of the present conception of sovereignty to the Treaty of Westphalia,[46] whereby states would agree not to intervene or interfere in the domestic affairs of another state. This notion of Westphalian sovereignty has been kept largely intact, and it

---

42 Samantha Beeson, "Sovereignty" (2011) Max Planck Encyclopedia of International Law. For a deeper interrogation between this concept of sovereignty and law, see *e.g.*, *Sovereignty and the Law: Domestic, European and International Perspectives* (Richard Rawlings, Peter Leyland, and Alison Young eds) (Oxford University Press, 2013).

43 Giovanni Distefano, *Fundamentals of Public International Law: A Sketch of the International Legal Order* (Brill Nijhoff, 2019) at p 89.

44 *Island of Palmas Case (Netherlands v USA)* (1925) 2 RIAA 829 at 838.

45 See *e.g.*, Christina Eckes, "The Reflexive Relationship between Internal and External Sovereignty" (2015) 18 Irish Journal of European Law 33 at 33; Samantha Beeson, "Sovereignty" (2011) Max Planck Encyclopedia of International Law.

46 James Crawford, *Brownlie's Principles of International Law* (Oxford University Press, 9th Ed, 2019) at p 4–6; Derek Croxton, "The Peace of Westphalia of 1648 and the Origins of Sovereignty" (1999) 21(3) The International History Review 569. For a historical overview of how the Treaty of Westphalia came about, see generally, Adam Watson, *The Evolution of International Society* (Routledge, 1992).

finds its legal expression, with modifications,[47] in Article 2(1) of the UN Charter,[48] which states that:

> "The Organization (United Nations) is based on the principle of the sovereign equality of all its Members."

B. Sovereignty in the cyberspace?

15 While sovereignty forms a fundamental tenet of the modern scheme of international law, how does it apply in the cyberspace? In John Perry Barlow's "Declaration of the Independence of Cyberspace" made in 1996, he claimed that states had "no sovereignty" in the realm of cyberspace.[49] In the earlier days of the conceptualisation of the cyberspace, objections were raised that sovereignty does not exist in the context of cyberspace since it exists as *res communis omnium* (*i.e.*, global commons),[50] aligned with the public perception that the internet is a metaphorical "Wild West".[51]

16 As Mueller argues, the rationale for such a conception of the cyberspace is that sovereignty cannot be nicely mapped onto the cyberspace. In the cyberspace, states can only regulate the way people subject to their authority (in the form of the physical devices and servers) access the "global cyberspace", but do not exercise supreme control over a "national cyberspace".[52] However, even if it is true that sovereignty is not exercised perfectly in the cyberspace, there are two main reasons why the *res communis* theory does not represent international law as applied in the cyberspace.

17 The first, is that a *res communis* view of cyberspace fails to give full weight to the necessary physical manifestation of cyberspace. While

---

47 Richard A Falk, "The Interplay of Westphalia and Charter Conceptions of the International Legal Order" in *The Future of the International Legal Order, Volume 1: Trends and Patterns* (Cyril E Black ed) (Princeton University Press, 1969) at p 33–70.

48 Charter of the United Nations (1945) 1 UNTS XVI.

49 John Perry Barlow, "A Declaration of the Independence of Cyberspace" (1996) Electronic Frontier Foundation <https://www.eff.org/cyberspace-independence>.

50 Mark Raymond, "Puncturing the Myth of the Internet as a Commons" (2013) 14 Georgetown Journal of International Affairs 53.

51 Sarah Mainwaring, "Always in Control? Sovereign States in Cyberspace" (2020) 5(2) European Journal of International Security 215 at 215–216.

52 Milton L Mueller, "Against Sovereignty in Cyberspace" 22(4) International Studies Review 779 at 790.

the cyberspace appears "ethereal and remain[s], for most, clouded in mystery",[53] it is undeniable that each and every piece of infrastructure that makes up the "cyberspace" is ultimately physical in nature. Servers, cables, computers, and the like which all make up the collective cyberspace, unlike other *res communis* such as outer space, exist within pre-existing state territories, and can be subject to the exercise of state sovereignty.[54]

18 This is closely linked to the second point, which is that for *res communis* to exist over the cyberspace, states must agree to forgo or give up claims of sovereignty which could have been exercised over it. For example, Franzese raised various examples such as the law of the sea, the law of outer space, and the law regulating the Antarctic, to argue that a *res communis* asset must necessarily be governed by a treaty with specific permissible uses, prohibitions, and boundaries where states agree to forgo, or leave unasserted claims of exclusive sovereignty.[55] While the requirement that treaty law should create the *res communis* is perhaps unnecessary (given that the characterisation of the high seas as *res communis* arose even before[56] the UN Convention on the Law of the Sea),[57] it still stands that such *res communis* can only come about where states parties agree to give up sovereign claims through rules of international law. In the context of the high seas, this was through a long-standing customary rule; yet there is no such customary rule in the cyberspace, nor is there any treaty which designates the cyberspace as part of the *res communis*. Apart from regional and bilateral agreements dealing with very specific areas of cyberspace, such as the Budapest Convention[58] which regulates cybercrime in mostly European states,[59] no comprehensive treaty dealing with all of cyberspace presently exists. Further, any claims that such a customary rule exists cannot be sustained.

---

53 Sean Watts & Theodore Richard, "Baseline Territorial Sovereignty and Cyberspace" (2018) 22(3) Lewis & Clark Law Review 771 at 780.

54 Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace" (2013) 89 International Law Studies 123 at 126–127.

55 Patrick W Franzese, "Sovereignty in Cyberspace: Can it Exist?" (2009) 64 Air Force Law Review 1 at 17.

56 See generally, Daniel P O'Connell, "Jurisdiction on the High Seas" in *The International Law of the Sea: Volume II* (Ivan A Shearer ed) (Oxford University Press, 1988).

57 Convention on the Law of the Sea (1982) 1833 UNTS 397.

58 Convention on Cybercrime (2001) ETS 185.

59 See also, the UN's plans for a new global treaty on cybercrime: UN General Assembly, "General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over 'Rushed' Vote at Expense of Further Consultations" (2021) UN Doc GA/12328.

Instead, the opposite is observed in various cyber-incidents that have occurred in recent years. In Chircop's analysis of such incidents, which include the 2014 hack of Sony Pictures by North Korea; the 2016 hack of the Democratic National Committee's servers during the US presidential election by Russia; and the 2017 ransomware attacks of Ukraine by Russia, he points out that the responses by the international community were one of condemnation. What these condemnations affirm is that many states do consider that sovereignty exists over cyberspace, which gives rise to the existence of certain rights.[60] Indeed, this is consistent with the positions taken by states such as China, Russia,[61] and France,[62] which have consistently asserted their state sovereignty in governing the cyberspace, rendering a treaty-based or a custom-based *res communis* regime unlikely in the near future.

C. Sovereignty as a primary rule?

19 Apart from the question of whether sovereignty does apply in the cyberspace or exists as *res communis*, there is also the important question of what "sovereignty" means in the cyberspace. Sovereignty as a legal principle is extremely broad, and many primary rules can properly fall under this wide umbrella, including the prohibition of the use of force and the obligation of non-intervention, which will be discussed below. However, apart from just being a legal principle, there is the important question of whether it is a distinct legal rule capable of being violated in the cyberspace. On one view, sovereignty is merely a legal principle, and not a primary rule capable of being violated. Amongst some of the proponents of this view are the United Kingdom and the United States. For example, the UK stated that:

> "… I am not persuaded that we can currently extrapolate from that general principle a specific rule

[60] Luke Chircop, "Territorial Sovereignty in Cyberspace after Tallinn Manual 2.0" (2019) 20(2) Melbourne Journal of International Law 349.

[61] President Xi Jinping & President Vladimir Putin, "The Joint Statement between the Presidents of the People's Republic of China and the Russian Federation on Cooperation in Information Space Development" (2016) *China Daily* <https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm>.

[62] Ministry for Europe and Foreign Affairs, "Paris Call for Trust and Security in Cyberspace" (2018) <https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf>.

> or additional prohibition for cyber activity beyond that of a prohibited intervention."[63]

On the other hand, the US stated that:

> "… The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."[64]

20 Even though the statements made by these parties may support the view that there is at present no primary rule of sovereignty in the context of the cyberspace (*i.e.*, that there is no customary prohibition against violating sovereignty by a state's actions in the cyberspace), that is not to say that there cannot be any primary rule of sovereignty that is capable of being violated. In essence, it is not that the rule of sovereignty is incapable of being violated; instead, these statements assert that there is insufficient state practice and *opinio juris* to make out any customary rule of sovereignty which applies specifically to the cyberspace.

21 Indeed, it is difficult to support the proposition that a primary rule of sovereignty cannot be violated in international law. This can be seen in the jurisprudence of the International Court of Justice, which has consistently accepted this position at law. A violation of sovereignty was, for example, made out in the *Certain Activities carried out by Nicaragua in the Border Area*,[65] where Nicaragua's excavation of three caños and

---

63 Attorney General Jeremy Wright, "Cyber and International Law in the 21st Century" (2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

64 Paul C Ney Jr, "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference" (2020) <https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>; see more recently, UN General Assembly, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States" (2021) UN Doc A/76/136. For a comparison between this statement and the UK's statement, see Russell Buchan, "When More is Less: The US Department of Defense's Statement on Cyberspace" (2020) *EJIL:Talk!* <https://www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/>.

65 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* (2015) ICJ Rep 665.

establishing a military presence in parts of the disputed territory was in violation of Costa Rica's territorial sovereignty.[66] In *Corfu Channel*,[67] the court also found that the United Kingdom violated the sovereignty of Albania through its mine clearing operations (Operation Retail).[68] So, too, did the court in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* consider the breaches of sovereignty as closely linked, but separate and distinct grounds of breach from the use of force and non-intervention.[69] There, the breach of sovereignty was made out by the following acts of the US: the US's assistance to the contras, the direct attacks on Nicaraguan ports and oil installations, the aerial overflights in Nicaragua,[70] and interference with the right of access to Nicaragua's ports through the US's mining of the ports.[71]

22 So, the important question that arises instead is whether there are sufficient *opinio juris* and state practice to support the position that sovereignty is a primary rule that can be violated. In addition to support for this proposition from Germany,[72] Finland,[73] and Iran,[74] this question was also answered in the affirmative by the *Tallinn Manual 2.0*. Formulated by independent experts under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence,[75] the *Tallinn Manual*

---

66 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)* (2015) ICJ Rep 665 at [229].

67 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4.

68 *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* (1949) ICJ Rep 4 at 36.

69 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [212].

70 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [251].

71 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [254].

72 Germany, "On the Application of International Law in Cyberspace: Position Paper" (2021) <https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>.

73 Finland, "International law and cyberspace: Finland's national positions" (2020) <https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727>.

74 Iran, "Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace" (2020) <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat>.

75 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 1.

2.0 sought to provide an objective statement of *lex lata*,[76] and is an important subsidiary means for determination of the rules of international law[77] in this nascent field of international law. Under the field of sovereignty, the experts expressed that sovereignty applied in the field of cyberspace and may be violated in two situations: (1) the degree of infringement upon the target state's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions.[78]

23 Beyond this level of generality, however, it is unclear what would constitute a breach of sovereignty. For the first situation, the factors that have been considered are whether the operations caused physical damage or injury, and whether it caused a loss of functionality of cyber infrastructure;[79] however, there has been no agreement on the exact standard that would constitute a breach of the primary rule.[80] For the latter, it is unclear what "inherently governmental functions" mean apart from extreme examples (*e.g.*, interference in the conduct of elections).[81]

IV. Other sovereignty-related rules

24 Apart from the primary rule of sovereignty, other rules of international law tightly linked to the principle of sovereignty would be implicated by cyberoperations conducted by a state. This includes the rule of non-intervention and the prohibition against the use of force.

---

76 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 31.

77 Statute of the International Court of Justice (1945) USTS 993, Article 38(1)(d).

78 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 20. See also, Michael N Schmitt & Liis Vihul, "Sovereignty in Cyberspace: *Lex Lata Vel Non*?" (2017) 111 AJIL Unbound 214.

79 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 20.

80 For the disagreements in the various standards on what amounts to a breach of sovereignty in the cyberspace, see *e.g.*, CCDCOE, "Sovereignty" <https://cyberlaw.ccdcoe.org/wiki/Sovereignty#:~:text=A%20State%20must%20not%20conduct,case%2Dby%2Dcase%20basis.>.

81 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 21.

A. Non-intervention

25 The rule of non-intervention is a customary rule which prohibits states from intervening in the internal or external affairs of other States. This rule is a "corollary of every state's right to sovereignty".[82] The rationale for this is obvious: a key element of sovereignty is the right of the state to choose its political, social, economic, and cultural systems, which "would be negatively affected if other States were entitled to intervene in such matters".[83]

26 A violation of this rule was most notably[84] made out in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*. There, the International Court of Justice laid out the standard for non-intervention, which is that:

> "A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely… [and] is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."[85]

27 The 1970 Friendly Relations Declaration,[86] which was an important document negotiated and adopted by consensus, similarly provides that:

> "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State."

---

82 Robert Y Jennings & Arthur D Watts, *Oppenheim's International Law* (Oxford University Press, 9th Ed, 2008) at p 428.

83 Dire Tladi, "The Duty Not to Intervene in Matters within Domestic Jurisdiction" in *The UN Friendly Relations Declaration at 50* (Jorge E Viñuales ed) (Oxford University Press, 2020) at p 90.

84 See also, the *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (2005) ICJ Rep 168 at [164]–[165], where the violation of the rule of non-intervention was also made out.

85 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [205].

86 UN General Assembly, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations* (1970) UN Doc A/RES/2625(XXV). See generally, *The UN Friendly Relations Declaration at 50* (Jorge E Viñuales ed) (Oxford University Press, 2020).

28 Such prohibition will not be made out if state practice justifies it. In the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, the court found that the US's support of the *contra* rebels violated the principle of non-intervention, which could not be justified by any state practice which illustrated a "belief in a kind of general right for States to intervene, directly or indirectly, with or without armed force, in support of an internal opposition in another State, whose cause appeared particularly worthy by reason of the political and moral values with which it was identified".[87]

29 Once again, the devil is in the details. Take for example, state X commencing fake news operations on the cyberspace against state Y to influence their elections in favour of candidate Z. Does it matter that this was an influence campaign against Y's elections? Does it matter that the news is fake? Does it matter that there is no physical damage caused by such operations? Does it matter that state Y has the technological capabilities to resist such influences? Would fake news be considered "influencing" or "factually compelling" state Y to act in a particular way? Would the fact that the fake news operations did not actually cause candidate Z to be elected mean that there is no coercion?

30 Indeed, while non-intervention is a customary rule, it is less clear *when* this rule would be violated in the cyberspace. To reframe the examples raised above between X and Y in legal terms, the main enquiry is whether the act of the state was an interference in the "internal affairs" of the state such that it would amount to "coercion" against the other state.

31 The "internal affairs" of a state derives from the concept of *domaine reserve*, which are matters "not, in principle, regulated by international law".[88] However, determining what properly falls within the *domaine reserve* of the state is a difficult task. As Kunig highlights, as "more problems fall into the sphere of international concern, fewer matters can be regarded as remaining purely domestic".[89] With

---

87 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [206].

88 *Nationality Decrees Issued in Tunis and Morocco (Advisory Opinion)* (1923) PCIJ (ser B) No 4 at 24.

89 Philip Kunig, "Intervention, Prohibition of" (2008) Max Planck Encyclopedia of Public International Law.

international law's increasing regulation of the cyberspace,[90] it becomes increasingly unclear what would constitute as "unregulated". Further complications arise where one considers the patchwork of international obligations that are subject to different states depending on their consent to these obligations, since what is regulated between two states may be left unregulated by others: the *Tallinn Manual* likewise acknowledges that the effect of such a patchwork is that there can be matters that are within the *domaine reserve*[91] of a state *vis-à-vis* some states and not others, depending on whether there is any rule of international law existing between the two parties that regulate that matter.[92]

32 There is also the question of how "coercion" is to be made out. The *Tallinn Manual* recognises this and observes that the distinction between "coercive and non-coercive cyber operations is not always clear".[93] For one, it is unclear whether the "coercive" act should have caused the outcome that was intended, or whether it is sufficient for the "coercive" act to be designed to change particular outcomes that are within the *domaine reserve* of the state. Further, would the capacity of the target state to resist any coercive actions be relevant to the question of whether the state had "coerced" the other state? For example, the *Tallinn Manual 2.0* proposed that coercion would be made out if it was "designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State".[94] Yet, on the contrary, Jamnejad and Wood have argued otherwise based on the *Friendly Relations Declaration*, that

[90] A clear example is the Budapest Convention on Cybercrime (2001) ETS 185, which creates a treaty regime for crimes committed via the internet. Other examples include the increasing application of human rights law to the cyberspace. See *e.g.*, Human Rights Committee, *General Comment 34* (2011) CCPR/C/GC/34 at [12]; more broadly. See Helen McDermott, "Application of the International Human Rights Law Framework in Cyber Space" in *Human Rights and 21st Century Challenges: Poverty, Conflict, and the Environment* (Dapo Akande *et al.* eds) (Oxford University Press, 2020).

[91] The Tallinn Manual distinguishes between "*domaine reserve*" and "domestic jurisdiction", preferring the usage of the term "*domaine reserve*" in the context of non-intervention: see *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 314.

[92] *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 316.

[93] *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 319.

[94] *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 318.

coercion would not be made out if "the pressure is such that it could reasonably be resisted".[95]

33 In addition, there may exist exceptions to the general rule, based on the mode of interference that a state engages in. For example, the *Tallinn Manual 2.0* postulates that coercion must be distinguished from "persuasion, criticism, public diplomacy, propaganda, retribution, mere maliciousness, and the like". It was reasoned that the distinction was because "such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State or seek no action on the part of the target State at all."[96]

34 However, with new technologies and different methods of influencing the masses abound, it becomes less clear if this distinction is tenable. Between government-funded botnets to flood the informational space with a particular political narrative in another state, to other forms of interferences such as fake news and deepfakes in other states, how do they differ from each other? Some have argued that the difference between them is the falsity of the information that is propagated—therefore, when considering Russia's actions during the 2016 US elections, Ohlin points out that despite common sense intuitions about its impropriety,[97] including the release of the Democratic National Congress's emails, the current legal framework of non-intervention (and sovereignty) cannot properly capture any wrongdoing of Russia.[98]

35 That being said, it is difficult to see how non-objective information through propaganda or flooding informational channels with a particular narrative would make it less "coercive" than fake news. Baade argues that fake news is coercive because rational decisions are made based on facts, and "the projection of a different set of facts [is coercive because it] constrains one's freedom to act by making certain options and conclusions no longer seem viable or making others seem

---

95 Jamnejad & Wood, "The Principle of Non-Intervention" (2009) 22(2) Leiden JIL 345 at 348.

96 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 318–319.

97 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" 95 Texas Law Review 1579 at 1580.

98 Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" 95 Texas Law Review 1579 at 1598.

mandatory".[99] In both cases, however, the crucial element is that of persuasion towards a particular goal that the interfering state engages in, which can exist at differing levels of intensity based on various factors such as the availability of information in the state, and the amount of funds being committed to such campaigns. Moreover, where the intensity of such influence campaigns is high and widespread in both cases, it would undoubtedly make certain options seem unviable; that one state uses fake news, and the other uses distorted news hardly changes this outcome. Perhaps what would be required to put such debates to rest is greater responses from states indicating their position on the matter to clearly delineate when interference becomes coercive in the cyberspace.

36 However, it is more settled that non-intervention would require more than a minor intrusion into a state's affairs. Indeed, an important reason for why sovereignty as a primary rule has met with some mixed reactions from states (as highlighted above), is that states often engage in low-intensity interferences, which can be hardly considered as violating international law.[100] Thus, some states worry that accommodating a separate rule of sovereignty may create a lower threshold than non-intervention, disrupting the present state of affairs, whereby common low-intensity interferences may even be considered a violation of international law. From the UK's BBC World Service which broadcasts across the globe, to South Korea's programming of broadcasts across the DMZ to North Korea, no state seriously claims that such actions would amount to a violation of international law.[101] Indeed, many have even gone so far as to consider cyber-espionage *per se* permissible under international law,[102] because of how widespread it is in today's world.[103] It is also in this light that any claim of non-intervention that arises from a state's cyberoperations needs to be

[99] Björnstjern Baade, "Fake News and International Law" 29(4) European Journal of International Law 1357 at 1364.

[100] Florian Kriener, "Cyber Space, Sovereignty and the Intricacies of International Law-Making: Reflections on Germany's Position Paper on International Law in Cyberspace" (2021) *Voelkerrechtsblog* <https://voelkerrechtsblog.org/cyber-space-sovereignty-and-the-intricacies-of-international-law-making/>.

[101] Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" 95 Texas Law Review 1579 at 1588.

[102] *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 19.

[103] *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 168–169.

viewed with circumspection, given the high threshold that needs to be met.

B. Use of force

37 The prohibition on the use of force is tightly connected to the rule of non-intervention and sovereignty; as Jamnejad and Wood observe, more is required to amount to a use of force than the rule of non-intervention, since it is a more "specific application of the principle of non-intervention, indeed the most important application of the principle."[104] This prohibition on the use of force is most prominently expressed in Article 2(4) of the UN Charter which was ratified after the horrors of the Second World War,[105] providing 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 in any other manner inconsistent with the Purposes of the United Nations."

38 As the UN Charter has been ratified by all 193 states, the prohibition on the use of force in Article 2(4) is widely accepted to reflect customary international law,[106] and widely considered to be a cornerstone of the UN system.[107]

39 The prohibition against the use of force has been a major point of contention in various cases before the International Court of Justice, including the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, *DRC v Uganda*,[108] and *Oil Platforms*[109] cases, as well as advisory opinions such as the *Nuclear Weapons Advisory*

---

104 Jamnejad & Wood, "The Principle of Non-Intervention" (2009) 22(2) Leiden JIL 345 at 348–49.

105 See generally, Justin Morris, "Origins of the United Nations" in *The Oxford Handbook on the United Nations* (Thomas G Weiss & Sam Daws eds) (Oxford University Press, 2nd Ed, 2018).

106 Michael Bothe, "Terrorism and the Legality of Pre-emptive Force" (2003) 14 European Journal of International Law 227 at 228.

107 *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (2005) ICJ Rep 168 at [148].

108 *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (2005) ICJ Rep 168.

109 *Oil Platforms (Islamic Republic of Iran v. United States of America)* (2003) ICJ Rep 161.

Opinion[110] and the *Wall Opinion*.[111] For example, in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, the court had the occasion to consider a host of actions that the US commenced against Nicaragua which was in alleged violation of this obligation. There, while the court considered that the laying of mines in early 1984 and attacks on Nicaraguan ports, oil installations and naval bases, and the arming and training of armed opposition forces[112] could constitute a use of force, the supply of funds to the *contra* rebels could not.[113] However, these would all amount to a violation of the rule of non-intervention.[114] As the jurisprudence of the court reveals, while the use of armed force by one state against another is a paradigmatic example of the use of force,[115] something short of the use of armed force (*i.e.*, the arming and training of opposition forces) would qualify. However, there is still the question of how to assess the threshold that must be met to qualify as a "use of force", since not all forms of intervention would.

40 Any attempts to reconcile this area of the law will have to answer the important question of the applicable model in comparing the scale and effects of a cyberoperation and a conventional use of force. As Roscini points out, there are three main models to compare them.[116] The first approach, the instrument-based approach, focuses on the means used to commit an act, which is ill-suited to the cyberspace since a malicious code will never look like conventional weapons.[117] The second, the target-based approach, focuses on the target of the operations, which is likewise ill-suited since there are often low-intensity interferences such as information collection which cannot properly be

[110] *Legality of the Threat or Use of Nuclear Weapons* (1996) ICJ Rep 226.
[111] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [251].
[112] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [247].
[113] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [228].
[114] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [228].
[115] UN General Assembly, *Definition of Aggression* (1974) UNGA Res 3314.
[116] Marco Roscini, "Cyber Operations as a Use of Force" in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias ed) (Edward Elgar, 2021) at p 236.
[117] Marco Roscini, "Cyber Operations as a Use of Force" in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias ed) (Edward Elgar, 2021) at p 236.

considered a use of force.[118] The third, which is the more commonly supported one,[119] is the effect-based approach, which focuses on the effects of the cyberoperations conducted by the state.[120]

41 Indeed, this approach was also adopted in the *Tallinn Manual 2.0*, where the experts adopted the approach of determining whether an action would amount to a use of force by the "scale and effects" test.[121] This test encapsulates a few non-exhaustive and non-legal criteria, which are: severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[122] To be clear, the "scale and effects" test was used in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* to determine if an act would meet the requisite threshold of an "armed attack" that would engage the inherent right to self-defence,[123] and the *Tallinn Manual 2.0*'s test represents an extension of this principle. An "armed attack" is clearly distinct from a "use of force", since in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua*, the court found that only the gravest form of the use of force would amount to an armed attack.[124] Nonetheless, adopting such a matrix to determine whether a use of force has occurred is sensible. This is because the scale and effects test can render any cyberoperation comparable to other more conventional forms of the use of force and

---

118 Marco Roscini, "Cyber Operations as a Use of Force" in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias ed) (Edward Elgar, 2021) at p 236.

119 Jason Barkham, "Information Warfare and International Law on the Use of Force" (2001) 34 New York University Journal of International Law and Politics 57 at 72; Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, 1981) at p 362–363.

120 Jason Barkham, "Information Warfare and International Law on the Use of Force" (2001) 34 New York University Journal of International Law and Politics 57 at 72; Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, 1981) at p 362–363.

121 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 330–331.

122 *Tallinn Manual 2.0* (Michael N Schmitt ed) (Cambridge University Press, 2017) at p 333–336.

123 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [195]. It must be noted that while Article 51 of the UN Charter provides for the right to inherent self-defence, this was not raised in that case because the US made a reservation to the jurisdiction of the court, such that the court could not hear matters relating to multilateral treaties (which included the UN Charter). See generally, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1984) ICJ Rep 392.

124 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)* (1986) ICJ Rep 14 at [191].

prevents the stultification of the prohibition against the use of force, since other models are inappropriate for nascent forms of technology, as argued above. Thus, for example, if the cyberoperations are conducted at a massive scale and result in physical effects such as bringing down a critical state infrastructure (*e.g.*, shutting down the power to a hospital), one can more readily draw parallels to conventional forms of the use of force, to conclude that the cyberoperations are similarly in violation of this international obligation.

42 A good example of what may amount to a use of force is the 2010 "Stuxnet" software which was built to undermine Iran's uranium enrichment facility. Allegedly built by Israel and the US, it sabotaged Iranian nuclear facilities by causing the centrifuges to spin out of control and destroy themselves. Putting aside questions of attribution, most have agreed that this was considered a use of force,[125] since the effects caused (*i.e.*, destruction of critical infrastructure) were similar to the effects of a conventional use of force.[126] The main difficulty with this approach is that it would represent an extension of the well-established principle of non-intervention, which existed way before the advent of cyberspace. Notwithstanding the support of this approach by academics, greater clarity should be sought to determine which approach would truly form part of the corpus of international law (either *via* proving *opinio juris* and state practice, or by the approach suggested by Judge Jessup which was elucidated above for the extension of established principles to other contexts).[127]

V. Conclusion

43 Due to the recent uptick in malicious cyberoperations, states have begun to adopt defensive measures to deal with this threat. In fact,

[125] See generally, Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina, "Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?" (2022) 7(1) Journal of Cyber Policy 97; David Weissbrodt, "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage" (2013) 22 Minnesota Journal of International Law 347 at 376; Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate" (2012) 67 Joint Force Quarterly 40.

[126] See also, Samuli Haataja & Afshin Akhtar-Khavari, "Stuxnet and International Law on the Use of Force: an Informational Approach" (2018) 7(1) Cambridge International Law Journal 99, for a different approach in analysing the Stuxnet attacks.

[127] See Part II of this article.

many states including Australia,[128] Korea,[129] the United Kingdom,[130] the United States, [131] Singapore, [132] have now instituted cyber-defence institutions to deal with this threat. But apart from sheer deterrence, an important arena for states to settle their disputes in a peaceful way is international law. Indeed, in this increasingly polarised world, it is in the realm of international law where states can properly make normative claims about the propriety of the actions of other states. However, because there lacks any sovereign in the Austinian sense,[133] or a world government, international law tends to be slow in catching up with new areas of development in the lack of any consensus. Thus, even while treaty law could, in theory, provide a rapid response to new problems, such agreement is hard to come by. Indeed, one needs to look no further than negotiations at the United Nations on the formulation of a new cybercrime treaty to see how a rapid response to new areas of the law may not be feasible, given the states' adoption of contrasting positions, and the need to negotiate extensively to reach agreeable solutions.[134]

44 Yet, not all is lost in protecting the sovereign rights of states in the cyberspace. As this paper has sought to show, despite the imperfect fit between the rules relating to sovereignty and cyberspace, it is not as if the cyberspace falls entirely outside the reach of international law and the sovereignty of states. Instead, what is required for this rule of sovereignty to be more robust in the context of cyberoperations is greater clarity, which may come in the form of independent judicial dispute

---

[128] Australian Government, "Information Warfare Division" <https://defence.gov.au/JCG/iwd.asp>.

[129] 법제처 (Ministry of Legislation, Korea), "사이버작전사령부령" <https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%9E%91%EC%A0%84%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9>.

[130] UK Ministry of Defence, "Working for UKStratCom" <https://www.gov.uk/government/organisations/strategic-command/about/recruitment>.

[131] United States Government, "US Cyber Command" <https://www.cybercom.mil/>.

[132] MINDEF Singapore, "Cyber Defence" <https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/cyber-defence>.

[133] John Austin, *The Province of Jurisprudence Determined* (Cambridge University Press, 1995).

[134] See *e.g.*, Deborah Brown, "Opening Stages in UN Cybercrime Treaty Talks Reflect Human Rights Risks" <https://www.hrw.org/news/2022/04/28/opening-stages-un-cybercrime-treaty-talks-reflect-human-rights-risks>; Joyce Hakmeh, "Can a cybercrime convention for all be achieved?" <https://www.chathamhouse.org/2022/03/can-cybercrime-convention-all-be-achieved>.

resolution mechanisms such as the Permanent Court of Arbitration or the International Court of Justice,[135] or even in states making their position on the law clearer to provide the *opinio juris* and state practice to form a specific customary rule on the matter.

[135] While decisions of these international judicial institutions are not formally binding as a source of international law, they are a subsidiary means of determining the rules of international law under Article 38(1)(d) of the Statute of the International Court of Justice and aid in the normative function of developing and stabilizing international law: see von Bogdandy & Venzke, "On the Functions of International Courts: An Appraisal in Light of Their Burgeoning Public Authority" (2013) 26(1) Leiden Journal of International Law; Gleider Hernandez, *The International Court of Justice and the Judicial Function* (Oxford University Press, 2014).