REINTERPRETING THE LEGALITY OF FORCIBLE SELF-DEFENCE IN RESPONSE TO NON-KINETIC CYBER ATTACKS

BEN HINES*

Article 51 of the Charter of the United Nations provides states who are subject to an armed attack the right to respond in self-defence through the use of force, a form of recourse prohibited in all other circumstances, absent Security Council authorisation, by art 2(4). Despite unequivocal agreement that the Charter of the United Nations applies to the cyber realm, there remains no consensus as to how arts 2(4) and 51 apply to cyber attacks. This uncertainty is significantly more pronounced vis-à-vis "non-kinetic" cyber attacks which do not manifest physically. Given the imperatives underpinning the ability to defend against ever-increasing cyber attacks which may have ramifications far greater than traditional weaponry, a novel approach is required. This article provides a bespoke framework to appropriately fill this lacuna, termed the "Substantive Necessity" approach. In arguing that notions of "force" and "gravity" do not have inherent requirements of physicality, it proposes that a non-kinetic cyber attack will amount to an "armed attack" animating the right to forcible self-defence where it is apprehended by the victim state based on clear and convincing evidence as a hostile act or set of acts which (a) has fundamentally compromised, or (b) is imminently poised to fundamentally compromise, the (i) functioning or (ii) security of (c) infrastructure crucial to a state's ability to function as such. This framework, it is argued, protects state interests and reinstates critical deterrents for aggressor states, yet crucially does not "open the floodgates" to enable the unacceptable escalation of unlawful force.

CONTENTS

* BCom, BAdvStud (Hons I, Medal), LLB (Hons I) (Syd); Tipstaff to the Hon Richard White, Justice of the New South Wales Court of Appeal; Sessional Academic at the University of Sydney. My sincere gratitude goes to Professor Ben Saul, Challis Chair of International Law at the University of Sydney and United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, for his invaluable feedback throughout the process of writing this article. I am also grateful to Dr Alison Pert for her constructive commentary on an earlier version, as well as for the feedback of two anonymous referees and the editorial team of the *Melbourne Journal of International Law*. All errors remain my own.

I INTRODUCTION

Quite unlike the milieu in which the *Charter of the United Nations*[1] ('*UN Charter*') was conceived and drafted, conflict in the 21st century is no longer confined to the visceral horrors of physical decimation to persons and property. The virtual realm, intuitively separate yet intimately connected with the "real world", is the 'new frontier of warfare' which 'any future conflict between reasonably advanced actors' will involve.[2] Technology is the bedrock of economies, infrastructure and governments. Perhaps then it is unsurprising that malicious acts between states have increasingly utilised cyberwarfare.[3] The capacity of states to generate substantial harm across the globe at the press of a

---

1 *Charter of the United Nations* Preamble ('*UN Charter*').

2 Nat Katin-Borland, 'Cyber War: A Real and Growing Threat' in Sean S Costigan and Jake Perry (eds), *Cyberspaces and Global Affairs* (Routledge, 2012) 3, 3. See also Espen Barth Eide and Anja Kaspersen, 'Cyberspace: The New Frontier in Warfare', *Agenda* (online, 24 September 2015) <https://www.weforum.org/agenda/2015/09/cyberspace-the-new-frontier-in-warfare/>, archived at <https://perma.cc/V4D9-MQCF>; United States Joint Forces Command, 'The Joint Operating Environment 2010' (Report, 18 February 2010) 36; Nick Heath, 'NATO Creates Cyber-Defence Command', *ZDNet* (online, 9 April 2008) <https://www.zdnet.com/article/nato-creates-cyber-defence-command/>, archived at <https://perma.cc/HMQ7-WFZ3>; Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17(2) *Journal of Conflict and Security Law* 187, 195.

3 Noah Simmons, 'A Brave New World: Applying International Law of War to Cyber-Attacks' (2014) 4(1) *Journal of Law and Cyber Warfare* 42, 44; Ido Kilovaty, 'Cyber Conflict and the Thresholds of War' in David L Sloss (ed), *Is the International Legal Order Unraveling?* (Oxford University Press, 2022) 251, 251; Oona A Hathaway et al, 'The Law of Cyber-Attack' (2012) 100(4) *California Law Review* 817, 837.

button has revolutionised modern conflict at a pace far outstripping the evolution of applicable legal frameworks.[4]

Prominent examples of (allegedly)[5] state-conducted cyber attacks can be found as early as 2007 and 2008, when Estonia[6] and Georgia[7] were the victims of widespread distributed denial-of-service ('DDoS') attacks, in response to conflict and as a prelude to war, respectively, which saw significant portions of the economy, media and government paralysed.[8] In 2010, the 'Stuxnet' worm, purportedly created by the United States and Israel, led to a serious nuclear accident which physically destroyed Iranian nuclear centrifuges.[9] In 2012, US

---

4 Priyanka R Dev, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response' (2015) 50(2–3) *Texas International Law Journal* 381, 382; Thomas Eaton, 'Self-Defense to Cyber Force: Combatting the Notion of "Scale and Effect"' (2021) 36(4) *American University International Law Review* 697, 698–9; Bradley Raboin, 'Corresponding Evolution: International Law and the Emergence of Cyber Warfare' (2011) 31(2) *Journal of the National Association of Administrative Law Judiciary* 602, 603; Scott J Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27(1) *Berkeley Journal of International Law* 192, 194; Cassandra M Kirsch, 'Science Fiction No More: Cyber Warfare and the United States' (2012) 40(4) *Denver Journal of International Law and Policy* 620, 622; Reese Nguyen, 'Navigating *Jus ad Bellum* in the Age of Cyber Warfare' (2013) 101(4) *California Law Review* 1079, 1098.

5 Cyber attribution presents significant challenges owing to various methods of creating anonymity online. Consequently, many cyber attacks see responsibility denied by states and a dearth of evidence with which to conclusively attribute culpability. However, in many instances it has been possible to identify perpetrators with reasonable certainty, and in any event the mere difficulty of attribution is no reason to dispense with the designation of such acts as illegal: Daniel B Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' (2002) 76 *International Law Studies* 73, 78; Russell Buchan and Nicholas Tsagourias, *Regulating the Use of Force in International Law* (Edward Elgar Publishing, 2021) 126.

6 Joshua Davis, 'Hackers Take Down the Most Wired Country in Europe', *Wired* (online, 21 August 2007) <https://www.wired.com/2007/08/ff-estonia>, archived at <https://perma.cc/L3FU-CZNS>; Stephen Herzog, 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses' (2011) 4(2) *Journal of Strategic Security* 49; Eaton (n 4) 703; Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News* (online, 27 April 2017) <https://www.bbc.com/news/39655415>, archived at <https://perma.cc/55KS-ZSTE>.

7 Lesley Swanson, 'The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict' (2010) 32(2) *Loyola of Los Angeles International and Comparative Law Review* 303, 303; Khatuna Burkadze, 'A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace' (2020) 44(1) *Fletcher Forum of World Affairs* 33, 37; Sandra L Hodgkinson, 'Crossing the Line' (2018) 51(3) *International Lawyer* 613, 615, 624.

8 Kilovaty (n 3) 258; Burkadze (n 7) 37; Davis (n 6); McGuinness (n 6).

9 James P Farwell and Rafal Rohozinski, 'Stuxnet and the Future of Cyber War' (2011) 53(1) *Survival* 23, 29; Kim Zetter, 'An Unprecedented Look at Stuxnet, the World's First Digital Weapon', *Wired* (online, 3 November 2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet>, archived at <https://perma.cc/ZV49-PB5C>; Ellen Nakashima and Joby Warrick, 'Stuxnet Was Work of US and Israeli Experts, Officials Say', *The Washington Post* (online, 2 June 2012) <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>, archived at <https://perma.cc/CR68-CX4A>.

banks were targeted by cyber operations,[10] and in 2021 cyber attacks described as 'nuclear terrorism' were conducted against Iranian electricity grids.[11] This listing is not to labour the point. In fact, it substantially understates the frequency of such occurrences.[12] With this trend only likely to continue,[13] questions must be asked as to the consequences of such acts under a *jus ad bellum* which, in its modern form, finds its origins in the early 20th century well before cyber attacks had even entered science fiction.[14]

Whilst the cyber age no doubt escaped the minds of the framers of the *UN Charter*,[15] it appears unequivocal that the relevant provisions — specifically here art 2(4)[16] prohibiting the use of force and art 51[17] permitting self-defence in limited circumstances — do *apply* to cyberspace.[18] Nonetheless, owing to scarce

---

10 Nicole Perlroth and Quentin Hardy, 'Bank Hacking Was the Work of Iranians, Officials Say', *The New York Times* (online, 8 January 2013) <https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html>, archived at <https://perma.cc/3JNC-9NBF>; Dev (n 4) 382; Daniel Campbell, 'Operation Ababil' in Nicholas Michael Sambaluk (ed), *Conflict in the 21st Century: The Impact of Cyber Warfare, Social Media, and Technology* (Bloomsbury Publishing, 2019) 65, 66.

11 Maziar Motamedi, 'Iran Calls Blackout at Natanz Atomic Site "Nuclear Terrorism"', *Al Jazeera* (online, 12 April 2021) <https://www.aljazeera.com/news/2021/4/11/incident-at-iranian-nuclear-site-targeted-by-blast-last-year>, archived at <https://perma.cc/9QW7-MDYG>; Gordon Corera, 'Iran Nuclear Attack: Mystery Surrounds Nuclear Sabotage at Natanz', *BBC News* (online, 13 April 2021) <https://www.bbc.com/news/world-middle-east-56722181>, archived at <https://perma.cc/8C7G-ZVKS>.

12 See, eg, 'Significant Cyber Incidents', *Center for Strategic and International Studies* (Web Page) <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>, archived at <https://perma.cc/KD3M-JRY5>.

13 Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 1(1) *Journal of Law and Cyber Warfare* 8, 18; Burkadze (n 7) 36; Kilovaty (n 3) 260.

14 Robert Kolb, 'Origin of the Twin Terms *Jus ad Bellum*/*Jus in Bello*' (1997) 37(320) *International Review of the Red Cross* 553, 553; Carsten Stahn, '"Jus ad Bellum", "Jus in Bello" ... "Jus post Bellum"?: Rethinking the Conception of the Law of Armed Force' (2006) 17(5) *European Journal of International Law* 921, 925; Lothar Kotzsch, 'The Concept of War in Contemporary History and International Law' (Librairie E Droz, 1956) 86; Cassandra M Kirsch, 'Science Fiction No More: Cyber Warfare and the United States' (2012) 40(4) *Denver Journal of International Law and Policy* 620, 646.

15 François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020) 277; Gervais (n 13) 27; Burkadze (n 7) 41.

16 *UN Charter* (n 1) art 2(4).

17 Ibid art 51.

18 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 68th sess, Agenda Item 94, UN Doc A/68/98 (24 June 2013) 8 [19]–[20] ('*UN Doc A/68/98*'); *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN GAOR, 70th sess, Agenda Item 93, UN Doc A/70/174 (22 July 2015) 12 [26] ('*UN Doc A/70/174*'). See also Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination, and the Principle of Non-Intervention in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield, 2020) 45, 45; Ma Xinmin, 'Key Issues and Future Development of International Cyberspace Law' (2016) 2(1) *China Quarterly of International Strategic Studies* 119, 128; Guiguo Wang, 'Are There International Rules Governing Cyberspace?' (2021) 8(2) *Journal of International and Comparative Law* 357, 370; Delerue (n 15) 277; Harold Hongju Koh, 'International Law in Cyberspace' (2012) 54 *Harvard International Law Journal Online* 1, 3; Michael N Schmitt, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty' (2013) 126(5) *Harvard Law Review Forum* 176, 177; Todd C Huntley, 'Controlling the Use of Force in Cyber Space: The Application of the Law of Armed Conflict during a Time of Fundamental Change in the Nature of Warfare' (2010) 60 *Naval Law Review* 1, 21.

jurisprudence and the infancy of state practice, the precise nature of this application remains subject to debate, particularly in situations where specific cyber attacks lack physical manifestations.[19] Agreement appears to be emerging that cyber attacks may in some circumstances amount to unlawful force,[20] but consensus as to what these circumstances are remains conspicuously absent.[21] Scholars tend to focus on attacks promulgating physical consequences akin to kinetic weaponry, being the destruction of property or physical injury, and generally agree that such acts will be forceful owing to the perceived severity of the physical effects.[22] "Non-kinetic" acts, being those which lack physical consequences — such as the crippling of financial institutions or the inhibition of vital government services — attract no such agreement.[23] It remains even less certain when, or indeed if, such cyber attacks may amount to "armed attacks" enlivening rights of self-defence.[24] The debate appears polarised between, on the one hand, expansive perceptions that all cyber attacks are armed attacks — which are largely linked to stances that argue that all force generally amounts to an armed attack[25] — and, on the other, a significantly restrictive emphasis on physicality which excludes non-kinetic attacks despite their potentially severe

---

19 Dev (n 4) 388.

20 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017) 328 ('*Tallinn Manual 2.0*'); Walter Gary Sharp Sr, *CyberSpace and the Use of Force* (Aegis Research Corporation, 1999) 5; Simmons (n 3) 51; Burkadze (n 7) 40.

21 Schmitt, *Tallinn Manual 2.0* (n 20) 332; Kilovaty (n 3) 263.

22 See Michael Kenney, 'Cyber-Terrorism in a Post-Stuxnet World' (2015) 59(1) *Orbis* 111. See also Anna Wortham, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2011) 64(3) *Federal Communications Law Journal* 643, 650–1; Wolff Heinegg von Heintschel, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies* 123, 128–9; Davis Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47(1) *Harvard International Law Journal* 179, 187; Marco Roscini, 'World Wide Warfare: *Jus ad Bellum* and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 85, 130; Schmitt, *Tallinn Manual 2.0* (n 20) 330–1.

23 Tsagourias (n 18) 3; Sean Watts, 'International Law and Proposed US Responses to the DNC Hack', *Just Security* (Blog Post, 14 October 2016) <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/>, archived at <https://perma.cc/Y6ZP-MEV4>; Duncan B Hollis, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention?', *Opinio Juris* (Blog Post, 25 July 2016) <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-nonintervention/>, archived at <https://perma.cc/4GN3-A7MD>; Brian J Egan, 'International Law and Stability in Cyberspace' (2017) 35(1) *Berkeley Journal of International Law* 169, 175.

24 Kilovaty (n 3) 263; Jackson Maogoto, *Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century* (Routledge, 2015) 57; Michael N Schmitt, 'The Law of Cyber Warfare: Quo Vadis' (2014) 25(2) *Stanford Law and Policy Review* 269, 275 ('The Law of Cyber Warfare').

25 See, eg, Abraham Sofaer, 'Address by: Abraham D Sofaer' (1988) 82 *Proceedings of the ASIL Annual Meeting* 420, 426; Office of General Counsel, Department of Defense (US), *Department of Defense Law of War Manual* (Manual, July 2023) 1030 [16.3.3.1]; Eaton (n 4) 699; Demitrios Delibasis, *The Right to National Self-Defence in Information Warfare Operations* (Arena Books, 2007) 131; Stephen Petkis, 'Rethinking Proportionality in the Cyber Context' (2016) 47(4) *Georgetown Journal of International Law* 1431, 1445–52.

consequences.[26] Neither approach is satisfactory. Questions also arise regarding whether cyber attacks should instead be considered unlawful on other grounds outside the *jus ad bellum*.[27]

Given the potentially devastating ramifications of non-kinetic cyber attacks, which may even surpass those of kinetic operations,[28] the imperatives of, in appropriate circumstances, permitting states to respond in self-defence appear clear.[29] This article therefore seeks to reinterpret the legality under the *jus ad bellum* of forcible self-defence in response to non-kinetic cyber attacks. It argues that cyber attacks, even those lacking physical consequences, may amount to both force and, more pertinently, armed attacks animating a right to self-defence. Despite an increased academic interest in this topic area in recent years, this article thus largely departs from the existing literature. It is part of a small minority proposing that sufficiently severe non-kinetic cyber attacks might suffice as armed attacks notwithstanding that they do not manifest physically.[30] Moreover, not only does it synthesise and detail existing perspectives in this area, but it is unique in proposing a normative framework for assessing such attacks rather than merely positing the *possibility* that such attacks might qualify or conflating all cyber force with cyber armed attacks.[31] In doing so, this article's framework is also eminently practical. Drawing on wider principles generally accepted under the *jus ad bellum* as well as recent state practice, it provides a standard against which states may assess cyber attacks in practice to determine if an armed attack has occurred. To this extent the framework does not necessarily seek to *define* a cyber armed attack per se, but instead to provide the indicia that such an attack has occurred.

The article's core propositions are as follows. Part II justifies focusing on the *jus ad bellum*, outlining that non-kinetic cyber attacks may be considered "force" before describing the applicable legal consequences of this characterisation as compared to other varieties of international illegality. Part III synthesises the existing legal landscape, describing traditional interpretations of the *UN Charter*

---

26 See, eg, Gary D Solis, *The Law of Armed Conflict: International Humanitarian Law in War* (Cambridge University Press, 3rd ed, 2022) 556; Nguyen (n 4) 1129; Vida M Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places' (2005) 51 *Naval Law Review* 132, 161; Hathaway et al (n 3) 841; Yoram Dinstein, 'Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference' (2013) 89 *International Law Studies* 276, 279.

27 Ashley Deeks, 'Defend Forward and Cyber Countermeasures' in Jack Goldsmith (ed), *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment* (Oxford University Press, 2022) 181, 186; Egan (n 23) 178; Michael N Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54(3) *Virginia Journal of International Law* 697, 699; Simmons (n 3) 68; Michael N Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (2011) 56(3) *Villanova Law Review* 569, 582 ('Cyber Operations').

28 Jakub Spáčil, 'Cyber Operations Against Critical Financial Infrastructure: A Non-Destructive Armed Attack?' (2022) 22(2) *International and Comparative Law Review* 27, 28; Matthew C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36(2) *Yale Journal of International Law* 421, 436.

29 Michael Preciado, 'If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure from Cyber Warfare' (2012) 1(1) *Journal of Law and Cyber Warfare* 99, 100–103. See Spáčil (n 28) 28; Maogoto (n 24) 15, 16.

30 See, eg, Spáčil (n 2829); Petkis (n 25) 1451; Simmons (n 3) 54; Ferry Oorsprong, Paul Ducheine and Peter Pijpers, 'Cyber-Attacks and the Right to Self-Defense: A Case Study of the Netherlands' (2023) 6(2) *Policy Design and Practice* 217, 228–9.

31 See above n 25.

and the jurisprudential lacuna relating to cyberwarfare. It contends that the reasoning of the International Court of Justice ('ICJ') has developed in contexts tied to physical warfare and that academic consideration of "gravity" has erroneously adopted a physical bent where contemporary state practice has not. Part IV argues that present academic approaches have failed to appropriately extend the law. It subsequently seeks to fill this lacuna by proposing that a non-kinetic cyber attack will amount to an "armed attack" animating the right to forcible self-defence where it is *apprehended by the victim state based on clear and convincing evidence as a hostile act or set of acts which (a) has fundamentally compromised, or (b) is imminently poised to fundamentally compromise, the (i) functioning or (ii) security of (c) infrastructure crucial to a state's ability to function as such*. It finally assesses this "Substantive Necessity" approach to conclude that it appropriately reinterprets the legality of forcible self-defence in response to non-kinetic cyber attacks.

II FORCING THE ISSUE? WHY THE *JUS AD BELLUM*

Despite the frequency of malicious cyber operations between states, the overwhelming balance of commentary argues that they are indeed unlawful, in one form or another, under international law.[32] Even where not suggesting such attacks amount to force, scholars have contended that where conducted by a hostile state[33] they breach rules of non-intervention,[34] violate state sovereignty,[35] infringe human rights[36] or if carried out on a state's territory indicate failure of 'due diligence'

---

32 Richard Suofade Ogbe, 'International Law, Cyber Crime and Crime of Aggression' (2023) 8 *African Journal of Criminal Law and Jurisprudence* 24, 27; Antonio Coco, Talita Dias and Tsvetelina van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) 33(4) *European Journal of International Law* 1275, 1279; Alexia Fitz and Richard L Wilson, 'Just Warfare: Is a Nuclear Attack an Appropriate Response to a Cyber Attack?' (2023) 18(1) *Proceedings of the 18th International Conference on Cyber Warfare and Security* 534, 536; Shan Ali and Sabira Naz Qureshi, 'Legal Framework of Right of Self Defense in Cyber Warfare: Application through Laws of Armed Conflict' (2022) 3(2) *Journal of Development and Social Sciences* 1076, 1079.

33 The application of the *jus ad bellum* to cyber attacks carried out by non-state actors is beyond the scope of this article, though is itself both complex and important. Given the significantly reduced barriers to entry as compared to traditional forms of conflict or warfare, the ability for non-state actors to carry out immensely harmful attacks through cyber means is significantly heightened.

34 Buchan and Tsagourias (n 5) 121–2; Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17(2) *Journal of Conflict and Security Law* 211, 214; Delerue (n 15) 193.

35 Delerue (n 15) 200; *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 66/24, 66th sess, 71st plen mtg, Agenda Item 93, UN Doc A/RES/66/24 (13 December 2011) para 4; *UN Doc A/68/98* (n 18) 8 [20]; Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace* (NATO Cooperative Cyber Defence Centre of Excellence, 2013) 189, 190; Andrey L Kozik, 'The Concept of Sovereignty as a Foundation for Determining the Legality of the Conduct of States in Cyberspace' (2014) 14 *Baltic Yearbook of International Law* 93, 99.

36 Delerue (n 15) 260; Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, 32nd sess, Agenda Item 3, UN Doc A/HRC/32/L.20 (27 June 2016) 3 [1]; *The Right to Privacy in the Digital Age*, GA Res 68/167, 68th sess, 70th plen mtg, Agenda Item 69(b), UN Doc A/RES/68/167 (21 January 2014) para 3.

obligations to suppress such activity.[37] We might then proceed on the assumption that cyber attacks are prohibited by international law, at which point the acerbic reader is minded to question just what this article seeks to achieve. Yet the bare claim "cyber attacks are already considered unlawful" neglects the fact that the consequences of each form of unlawfulness differ significantly.[38] This article argues that non-kinetic cyber attacks are specifically illegal under the *jus ad bellum* as prohibited force which if sufficiently grave may amount to armed attacks.

A *Can Non-Kinetic Cyber Attacks Ever Be "Force"?*

Before tackling the self-defence issue, one must first deal with the threshold question of whether cyber attacks which do not cause physical harm can ever amount to "force" under art 2(4) of the *UN Charter*.[39] A negative answer would be fatal to the proposition that they could be responded to forcibly in self-defence.

1 *Defining "Non-Kinetic Cyber Attacks"*

The term "cyber attack" lacks a universal formal definition and is often used interchangeably with, or alongside, similar terms such as "cyber operation" or "cyber warfare".[40] Looking, however, to various informative definitional sources,

---

[37] Delerue (n 15) 211; James A Green, 'Disasters Caused in Cyberspace' in Susan C Breau and Katja LH Samuel (eds), *Research Handbook on Disasters and International Law* (Edward Elgar Publishing, 2016) 406, 412, 418; Catherine Lotrionte, 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights' (2012) 26(2) *Emory International Law Review* 825, 854; Schmitt (n 24) 276.

[38] See generally Russell Buchan, 'Non-Forcible Measures and the Law of Self-Defence' (2023) 72(1) *International and Comparative Law Quarterly* 1, 2; Yarik Kryvoi, 'Responding to Public and Private Cyberattacks: Jurisdiction, Self-Defence, and Countermeasures' in Tomoko Ishikawa and Yarik Kryvoi (eds), *Public and Private Governance of Cybersecurity: Challenges and Potential* (Cambridge University Press, 2023) 103; Michael N Schmitt, 'Cyber Activities and the Law of Countermeasures' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence, 2013) 659, 662; Robin Geiß and Henning Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention' in Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence, 2013) 621, 629–32.

[39] *UN Charter* (n 1) art 2(4). See also Petkis (n 25) 1446; Buchan and Tsagourias (n 5) 114; Dev (n 4) 395.

[40] Burkadze (n 7) 35; Hathaway et al (n 3) 881; Enenu Onyikwu Okwori, 'Cyber-Attacks as an Emerging Use of Force under International Law' (2022) 11 *Aberdeen Student Law Review* 33, 36; Medhi Kadivar, 'Cyber-Attack Attributes' [2014] (November) *Technology Innovation Management Review* 22, 23; Vasile Coman, 'Cyber Aggression in Conditions of Armed Conflict: Regulation and Counteraction' (2023) 24(133) *Romanian Journal of Forensic Science* 84, 86; Paul AL Ducheine and Peter BMJ Pijpers, 'The Notion of Cyber Operations' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2021) 272; Max Smeets and JD Work, 'Operational Decision-Making for Cyber Operations: In Search of a Model' (2020) 5(1) *Cyber Defense Review* 95.

provided both by states[41] and scholars,[42] there appears to be a general understanding of the ambit of acts to which the term refers alongside several consistently cited indicia. Generally, a cyber attack will involve (i) the use of computers or computer networks, (ii) action taken against or coopting the computers or computer networks of the target and (iii) 'hostile' intent.[43] This characterisation is not intended to be authoritative[44] but suffices for present purposes.

Cyber attacks are often understood through examples or categories.[45] A simple example is a DDoS attack, where thousands of computers are coopted remotely to overwhelm servers with traffic which prevents their function.[46] Meanwhile, malware is a broad category of software which hijacks computer systems, including viruses, worms and Trojan horses.[47] Phishing and spoofing involve attackers soliciting sensitive information by posing as legitimate sources or individuals.[48] Hacking or domain name system ('DNS') tunnelling involves gaining access to the target's network, enabling retrieval of information or control

---

41 Vice Chairman of the Joint Chiefs of Staff (US), 'Joint Terminology for Cyberspace Operations' (Memorandum, November 2010) 5; 'How Cyber Attacks Work', *National Cyber Security Centre* (Web Page, 14 October 2015) <https://www.ncsc.gov.uk/information/how-cyber-attacks-work>, archived at <https://perma.cc/PDV9-LM54>; 'Cyber Attack', *Australian Signals Directorate* (Web Page) <https://www.cyber.gov.au/glossary/cyber-attack>, archived at <https://perma.cc/3CLJ-Y7E2>.

42 See, eg, Schmitt, *Tallinn Manual 2.0* (n 20) 452; Hathaway et al (n 3) 821; William A Owens, Kenneth W Dam and Herbert S Lin (eds), *Technology, Policy, Law, and Ethics regarding US Acquisition and Use of Cyberattack Capabilities* (National Academies Press, 2009) 10–11; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014) 17 ('*Cyber Operations*'); M Uma and G Padmavathi, 'A Survey on Various Cyber Attacks and Their Classification' (2013) 15(5) *International Journal of Network Security* 390, 390; Waxman (n 28) 422.

43 Kadivar (n 40) 23.

44 Nor need it be, for in practice the issue of whether an act is a "cyber attack" under a formal definition appears unlikely to cause issues for states.

45 See, eg, TR Shejin and KT Sudheer, 'A Review on Major Cyber Threats and Recommended Counter Measures' (2023) 11(3) *International Journal for Research in Applied Science and Engineering Technology* 1758, 1760.

46 See Jose Nazario, 'Politically Motivated Denial of Service Attacks' in Christian Czosseck and Kenneth Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, 2009) 163; Sherwin Kati et al, 'Comprehensive Overview of DDOS Attack in Cloud Computing Environment Using Different Machine Learning Techniques' (Conference Paper, International Conference on Innovative Computing and Communication, 19–20 April 2022); 新华社 [Xinhua News Agency], « 北京警方专项打击网络攻击违法犯罪抓获嫌疑人379名» [Beijing Police Specifically Cracked Down on Illegal and Criminal Cyberattacks, Arresting 379 Suspects], *中华人民共和国中央人民政府* [*Central People's Government of the People's Republic of China*] (Web Page, 17 December 2019) <https://www.gov.cn/xinwen/2019-12/17/content_5461787.htm> [tr author], archived at <https://perma.cc/U54V-KB47>.

47 Petkis (n 25) 1445.

48 Elmer EH Lastdrager, 'Achieving a Consensual Definition of Phishing Based on a Systematic Review of the Literature' (2014) 3 *Crime Science* 9:1–10, 8; Huajun Huang, Junshan Tan and Lingxi Liu, 'Countermeasure Techniques for Deceptive Phishing Attack' (Conference Paper, International Conference on New Trends in Information and Service Science, 30 June – 2 July 2009) 636–7.

of function.[49] This list is not exhaustive but is indicative of acts I shall consider "cyber attacks" for the purposes of this article. As can be seen, each example and category reflects the indicia described above.

In defining which cyber attacks are "non-kinetic", one looks to their outcome. Whilst some uses of the above forms of cyber attack may manifest in physical harm — such as the Stuxnet virus causing physical destruction of centrifuges by causing them to spin too quickly via their computer control systems[50] — a non-kinetic attack is circumscribed to the cyber realm.[51] It has no *physical* manifestation as 'destructive or injurious' damage.[52] It may corrupt data or prohibit computer functions, for example, in some cases to devastating effect,[53] yet any harm is not a direct kinetic result of the attack.

Prominent examples of the consequences of such attacks might include data theft, economic losses, disruption to cyber systems, disruption of infrastructure reliant on such cyber systems, national security threats, misinformation and much more. Of course, in defining whether a cyber attack is kinetic or non-kinetic one must draw a clear chain of causality: to the extent an effect is primarily precipitated because of the cyber attack it is an effect of that cyber attack which may define whether the attack itself is physical or non-physical. If secondary effects are necessary and natural consequences of the specific attack — for example, the physical destruction of centrifuges by Stuxnet as a secondary result of the virus speeding up their operation — then the attack is kinetic. Conversely, if any physical consequences are not the direct result of the effect of the operation — for example, an inability to operate on a patient due to power outages caused by a cyber attack — then the attack itself remains non-kinetic.

2 *"Force" under the UN Charter*

Having defined "non-kinetic" cyber attacks, their inclusion within the *jus ad bellum* becomes contingent on whether "force" as contemplated by art 2(4) of the *UN Charter* definitionally excludes acts which are not physical in nature, no matter the severity of their non-physical impact. It appears that the dominant view within the literature is that cyber attacks which manifest in physical harm comparable to that caused by traditional weaponry prima facie may amount to force owing to

---

49 David J Gunkel, *Hacking Cyberspace* (Westview Press, 2001) 2–4; Tim Jordan, 'A Genealogy of Hacking' (2017) 23(5) *Convergence* 528, 535; DeJarvis Oliver and Adriane B Randolph, 'Hacker Definitions in Information Systems Research' (2022) 62(2) *Journal of Computer Information Systems* 397, 403; Yue Wang et al, 'A Comprehensive Survey on DNS Tunnel Detection' (2021) 197 *Computer Networks* 108322:1–19, 1.

50 Sean Collins and Stephen McCombie, 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications' (2012) 7(1) *Journal of Policing, Intelligence and Counter Terrorism* 80, 85; Ivanka Barzashka, 'Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme' (2013) 158(2) *RUSI Journal* 48, 50–1.

51 Martti Lehto and Gerhard Henselmann, 'Non-Kinetic Warfare: The New Game Changer in the Battle Space' in Brian K Payne and Hongyi Wu (eds), *Proceedings of the 15th International Conference on Cyber Warfare and Security* (Academic Conferences and Publishing International, 2020) 316, 318; Rob Schrier, 'COVID-19 and Cyber: Foreshadowing Future Non-Kinetic Hybrid Warfare' (2021) 6(2) *Cyber Defense Review* 29, 32–3; Schmitt 'The Law of Cyber Warfare' (n 24) 279; Preciado (n 29) 107.

52 Schmitt, 'The Law of Cyber Warfare' (n 24) 279.

53 Such as undermining critical medical infrastructure.

their physical consequences.[54] This article shall not retread this ground. However, as outlined, there remains 'significant uncertainty' as to whether non-kinetic cyber attacks may definitionally amount to unlawful "force".[55]

The foundational principles underlying the *UN Charter* are decidedly anti-force.[56] Article 2(4), a 'cornerstone' of the *UN Charter*,[57] provides the 'central rule on the use of force':[58] 'All Members shall refrain in their international relations from the threat or use of force'.[59]

Despite such foundational and even *jus cogens* status,[60] the definition of force lacks consensus,[61] a problem no doubt exacerbated by a lack of formal definition within the *UN Charter*.[62] A not-insignificant proportion of scholars has, it is

---

54 Petkis (n 25) 1447; Hathaway et al (n 3) 842; Solis (n 26) 556; Buchan and Tsagourias (n 5) 118; Schmitt, 'The Law of Cyber Warfare' (n 24) 279; Green (n 37) 413.

55 Green (n 37) 413.

56 *UN Charter* (n 1) arts 1, 2(4), 51. See also Franklin Berman, 'The UN Charter and the Use of Force' (2006) 10 *Singapore Year Book of International Law* 9, 10; John C Yoo, 'Force Rules: UN Reform and Intervention' (2006) 6(2) *Chicago Journal of International Law* 641, 643.

57 *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment)* [2005] ICJ Rep 168, 223 [148] ('*Armed Activities*'); Carlos Tünnermann Bernheim, 'United States Armed Intervention in Nicaragua and Article 2(4) of the United Nations Charter' (1985) 11(1) *Yale Journal of International Law* 104, 104; Ido Kilovaty, 'Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter' (2015) 4(3) *Journal of Law and Cyber Warfare* 210, 227; Yoram Dinstein, 'Computer Network Attacks and Self-Defense' in Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, 2002) 99, 99; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th ed, 2012) 719.

58 Christine Gray, *International Law and the Use of Force* (Oxford University Press, 4th ed, 2018) 32; Rachel Buckman, 'Expansive Application of Self-Defence: Protecting Security at the Expense of Legality' (2019) 17(2) *New Zealand Journal of Public and International Law* 153, 155–6.

59 *UN Charter* (n 1) art 2(4).

60 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14, 100 [190] ('*Nicaragua*'); Schmitt, *Tallinn Manual 2.0* (n 20) 331; Gray (n 58) 32; Kamrul Hossain, 'The Concept of Jus Cogens and the Obligation under the UN Charter' (2005) 3(1) *Santa Clara Journal of International Law* 72, 89; Sondre Torp Helmersen, 'The Prohibition of the Use of Force as *Jus Cogens*: Explaining Apparent Derogations' (2014) 61(2) *Netherlands International Law Review* 167, 173; Olivier Corten and Vaios Koutroulis, 'The *Jus Cogens* Status of the Prohibition on the Use of Force: What Is Its Scope and Why Does It Matter?' in Dire Tladi (ed), *Peremptory Norms of General International Law (Jus Cogens): Disquisitions and Disputations* (Brill, 2021) 629, 629.

61 Delerue (n 15) 279.

62 Tom Ruys, 'The Meaning of Force and the Boundaries of the *Jus ad Bellum*: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?' (2014) 108(2) *American Journal of International Law* 159, 163 ('The Meaning of Force'); Brian L Cox, 'The Risk of Obsolescence: Reframing the Contemporary Use of Force Model to Achieve a More Holistic Application of the *UN Charter Jus ad Bellum* Construct' (2021) 58 *Canadian Yearbook of International Law* 263, 299; Tomohiro Mikanagi, 'Establishing a Military Presence in a Disputed Territory: Interpretation of Article 2(3) and (4) of the UN Charter' (2018) 67(4) *International and Comparative Law Quarterly* 1021, 1023; Coman (n 40) 85; Buchan and Tsagourias (n 5) 119–20; Preciado (n 29) 132.

acknowledged, argued that force refers to armed or physical force.[63] Yet art 2(4) does not refer to physical or armed force.[64] This distinction is telling:[65] all other provisions in the *UN Charter* which refer to force, except art 44 which may be read as referring to art 2(4),[66] speak of 'armed force'.[67] The absence of the qualifier in art 2(4) implies the provision may be read more widely,[68] having been left 'vague' to capture sufficiently harmful conduct that was not explicitly conceived of at the time of drafting.[69] Recourse to the *UN Charter*'s *travaux préparatoires*[70] reveals an intent 'to state in the broadest terms an absolute all-inclusive prohibition … [to prevent any] loopholes'.[71] It also reflects the ICJ's declaration that the *UN Charter* applies to 'any use of force, regardless of the weapons employed'.[72]

Accepting that there is a 'cascading relationship'[73] between force, aggression and armed attack, it is telling that the UN General Assembly's *Definition of Aggression* considers acts including blockades and the acquiescence to the use of territory as 'aggression' when the 'consequences' of such acts are plainly not *physical*.[74] Even if these acts are argued as possessing a kinetic element — such

---

63 Eaton (n 4) 727; Ruys, 'The Meaning of Force' (n 62) 163; Oorsprong, Ducheine and Pijpers (n 30) 220; Tom J Farer, 'Political and Economic Coercion in Contemporary International Law' (1985) 79(2) *American Journal of International Law* 405, 407–8; Oscar Schachter, 'The Right of States to Use Armed Force' (1984) 82(5–6) *Michigan Law Review* 1620, 1624; Heather Harrison Dinnis, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) 40–1; Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press, 1963) 362; Preciado (n 29) 132–3; Tom Ruys, *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press, 2010) 55 ('*"Armed Attack" and Article 51*').

64 *UN Charter* (n 1) art 2(4). See also Buchan and Tsagourias (n 5) 22. Cf *Report of the Independent International Fact-Finding Mission on the Conflict in Georgia: Volume II* (Report, September 2009) 242.

65 Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press, 2020) 24, 24; Lianne JM Boer, '"Echoes of Times Past": On the Paradoxical Nature of Article 2(4)' (2015) 20(1) *Journal of Conflict and Security Law* 5, 11.

66 *UN Charter* (n 1) art 44. See also Murray Colin Alder, *The Inherent Right of Self-Defence in International Law* (Springer, 2013) 82; Nico Schrijver, 'Challenges to the Prohibition to Use Force: Does the Straitjacket of Article 2(4) UN Charter Begin to Gall Too Much?' in Niels Blokker and Nico Schrijver (eds), *The Security Council and the Use of Force: Theory and Reality – A Need for Change?* (Martinus Nijhoff Publishers, 2005) 31, 34.

67 *UN Charter* (n 1) Preamble, arts 41, 46.

68 Delerue (n 15) 287.

69 Boer (n 65) 11; James A Delanis, 'Force under Article 2(4) of the United Nations Charter: The Question of Economic and Political Coercion' (1979) 12(1) *Vanderbilt Journal of Transnational Law* 101, 109.

70 As permitted by the *Vienna Convention on the Law of Treaties*, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980) art 32 ('*VCLT*').

71 *Summary Report of Eleventh Meeting of Committee I* (Documents of the United Nations Conference on International Organization, San Francisco, 1945) vol 6, 334, 335; Thomas M Franck, *Recourse to Force: State Action against Threats and Armed Attacks* (Cambridge University Press, 2002) 12.

72 *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ Rep 226, 244 [39] ('*Nuclear Weapons*').

73 Ruys, 'The Meaning of Force' (n 62) 162. See also Claus Kreß, '"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice' (2013) 83(1) *British Yearbook of International Law* 160, 162; Delerue (n 15) 276; *Definition of Aggression*, GA Res 3314 (XXIX), UN GAOR, 2319th plen mtg, UN Doc A/RES/3314(XXIX) (14 December 1974) annex ('*Definition of Aggression*').

74 See, eg, *Definition of Aggression* (n 73) annex arts 3(c), 3(f), 3(g).

as existing physically as a *show* or *threat*[75] of physical force[76] — they still do not create physical *consequences*.[77] Indeed, this is consistent with ICJ jurisprudence, which has 'rejected a narrow interpretation … [limiting] the term to … kinetic force'.[78] As states continue to witness the significant harm non-kinetic cyber attacks may cause, there appears nascent acceptance in the literature of their status as at least prohibited "force".[79]

Yet still, despite these perspectives, requirements of physicality remain a schism in the scholarship.[80] This article posits that eschewing physical requirements and deeming non-kinetic cyber attacks as capable of amounting to force is the more appropriate position to adopt as a matter of law and in practice. The legal argument has already been canvassed, but it is also pragmatically prudent to note that neglecting to adopt such perspectives would produce 'illogical' outcomes where cyber attacks that might 'jeopardise the survival of the targeted state' would not even amount to "force", *let alone* armed attacks capable of permitting self-defence.[81]

3 *Rejection of Economic Coercion*

At the point at which it is accepted that physicality is not a prerequisite for "force", it appears the largest legal hurdle to considering non-kinetic attacks as forcible is the contention that they nonetheless intrinsically better reflect economic coercion, which is not prohibited by art 2(4) of the *UN Charter* and cannot amount to an "armed attack".[82] It is imperative, therefore, to outline why non-kinetic cyber attacks are distinct from so-called "economic coercion".

After significant debate in the latter half of the 20th century, it is now generally accepted that acts of economic coercion — commonly considered to refer to acts undertaken by one state which indirectly seek to induce specific acts from another state by harming it economically,[83] such as 'trade restrictions, … embargoes and

---

75 Yet blockades are themselves considered to be forceful, rather than enlivening the limb of art 2(4) of the *UN Charter* which prohibits the 'threat' of force. Moreover, examples such as acquiescence as described above would not enliven art 2(4) as a 'threat' as no such threat can be inferred from such action: ibid.

76 Eaton (n 4) 739.

77 Burkadze (n 7) 40.

78 Ibid 39; Schmitt, 'The Law of Cyber Warfare' (n 24) 279.

79 See, eg, Yoram Dinstein, *War, Aggression and Self-Defence* (Cambridge University Press, 5th ed, 2011) 88; Delerue (n 15) 296–8; Michael Schmitt and Jeffrey Biller, 'The NotPetya Cyber Operation as a Case Study of International Law', *EJIL: Talk!* (Blog Post, 11 July 2017) <https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/>, archived at <https://perma.cc/RV3Y-ZV4S>.

80 Antolin-Jenkins (n 26) 155; Green (n 37) 413.

81 Delerue (n 15) 298.

82 William Banks, 'The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare' (2013) 89 *International Law Studies* 157, 166; Green (n 37) 413; Stephenie Gosnell Handler, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48(1) *Stanford Journal of International Law* 209, 226–9.

83 Richard B Lillich, 'Economic Coercion and the International Legal Order' (1975) 51(3) *International Affairs* 358, 361–2; EY Benneh, 'Economic Coercion, the Non-Intervention Principle and the Nicaragua Case' (1994) 6(2) *African Journal of International and Comparative Law* 235, 239; Farer (n 63) 408; Antonios Tzanakopoulos, 'The Right to be Free from Economic Coercion' (2015) 4(3) *Cambridge Journal of International and Comparative Law* 616, 617.

other economic sanctions'[84] — do not fall afoul of art 2(4).[85] Whilst such measures may otherwise violate international law, this "indirect force" does not violate the *jus ad bellum*. The argument is that coercion aims to influence the acts of a state as with force, but unlike the latter it is indirect and only *pressuring*, rather than *forcing* directly.[86]

The taxonomical distinction between force and coercion has significantly informed academic reticence to consider non-kinetic cyber attacks as unlawful force.[87] Indeed, parallels between non-kinetic cyber attacks and economic coercion certainly exist, especially as both lack physical manifestation in the way that "force" as traditionally conceived possesses. If, therefore, non-kinetic cyber attacks were considered more akin to coercion than force, then the ability to respond in self-defence would be precluded and this article moot. This article argues, however, that non-kinetic cyber attacks may readily be distinguished from coercion.

Non-kinetic cyber attacks are better characterised as violently *forcing* rather than *pressuring* action.[88] A cyber attack wiping out a stock exchange is more akin, in terms of *mechanisms* by which the relevant consequences are imparted, to a kinetic bombardment which attacks by decimating the building it is contained in, thus directly preventing its function, than to an economic sanction undermining the economy as a whole and indirectly impairing the exchange.[89] Further, in many instances a cyber attack is not even "economic" in nature.[90] An attack shutting down power grids mirrors the outcome of their physical destruction — being an inability to function — rather than any economic coercion.[91] Even if economic harm stems from this cyber attack, it is secondary, being a derivative consequence of the physical shutdown rather than of the attack itself, and one which would also occur if the attack were physical. As Lianne JM Boer notes, economic coercion

---

84 *Economic Measures as a Means of Political and Economic Coercion Against Developing Countries*, GA Res 42/173, UN GAOR, 42nd sess, 96th plen mtg, UN Doc A/RES/42/173 (11 December 1987) para 3.

85 Spáčil (n 29) 34; Dev (n 4) 387; Farer (n 63) 413; Oliver Dörr and Albrecht Randelzhofer, 'Purposes and Principles: Article 2(4)' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary* (Oxford University Press, 3rd ed, 2012) 200, 208–10; Preciado (n 29) 133.

86 Christian Payne and Lorraine Finlay, 'Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack' (2017) 49(3) *George Washington International Law Review* 535, 546.

87 Buchan (n 38) 224–7; Herbert S Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4(1) *Journal of National Security Law and Policy* 63, 80; Huseyin Kuru, 'Prohibition of Use of Force and Cyber Operations as "Force"' (2017) 2(2) *Journal of Learning and Teaching in Digital Age* 46, 52.

88 Ekow N Yankah, 'The Force of Law: The Role of Coercion in Legal Norms' (2008) 42(5) *University of Richmond Law Review* 1195, 1216, 1218; Ignaz Seidl-Hohenveldern, 'The United Nations and Economic Coercion' (1984–85) 18(1) *Revue Belge de Droit International* [Belgian Review of International Law] 9, 11.

89 Preciado (n 29) 135.

90 Wolfgang McGavran, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 *Tulane Journal of Technology and Intellectual Property* 259, 260; Jordan J Plotnek and Jill Slay, 'Cyber Terrorism: A Homogenized Taxonomy and Definition' (2021) 102 *Computers and Security* 102145:1–9, 5.

91 Council on Foreign Relations, *A Cyberattack on the US Power Grid* (Memorandum, April 2017) 3; Dev (n 4) 396; James E McGhee, 'Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy' (2013) 2(1) *Journal of Law and Cyber Warfare* 64, 100; Delerue (n 15) 269.

and force are 'not ends to the same continuum',[92] with the former definitionally contingent on economic means.

A further important distinction is the definitional function of "intent" within coercion. Oftentimes, an act considered coercion, such as a decision to not trade with a state, would be legally permissible absent coercive intent.[93] The same is not true of acts comprising cyber attacks. Finally, acts traditionally considered as coercion often "exist" as a decision made within the "coercing" state, and the act or omission is "carried out" as such.[94] A trade embargo requires no interference directly with the "coerced" state, even where its effects are *felt* in said state. A cyber attack, meanwhile, interferes with the systems of the victim state *within* the victim state; whilst the push of the button may occur at home, the cyber attack "exists" not in the location of the initial act, but abroad.[95]

Non-kinetic cyber attacks can therefore be readily distinguished from coercion. The consequences of this distinction are twofold. First, non-kinetic cyber attacks are not thus excluded from the *jus ad bellum* and, second, their inclusion therein will not impermissibly broaden "force" to capture previously excluded coercion.[96]

B *Ramifications*

Having seen that it is *possible* to consider non-kinetic cyber attacks under the *jus ad bellum*, we turn to the normative desirability of such an approach at law.

1 *Force*

If non-kinetic cyber attacks are considered as potentially forceful, the primary consequence is, of course, that they are prohibited by art 2(4) of the *UN Charter*. This coincides with the jurisprudential, practical, and normative consequences described above, and their use shall violate the express prohibition found in that provision. It also leads to a number of further consequences. Consideration of non-kinetic cyber attacks as acts which may amount to prohibited force prevents their use as legitimate[97] countermeasures between states. Whilst states may utilise

---

92 Boer (n 65) 16.

93 See, eg, Mohamed S Helal, 'On Coercion in International Law' (2019) 52(1) *New York University Journal of International Law and Politics* 1, 104–8; Marko Milanovic, 'Revisiting Coercion as an Element of Prohibited Intervention in International Law' (2023) 117(4) *American Journal of International Law* 601, 630; Schmitt, 'The Law of Cyber Warfare' (n 24) 275. The role of intent in such a characterisation is also demonstrated in case law. For example, whilst a trade embargo with a coercive intent to induce a change in policy may violate the principle of non-intervention, the decision to cease trading with a state absent such intent may be permissible: *Nicaragua* (n 60) 115–16 [244]–[245]. Moreover, the ICJ in *Nicaragua* (n 60) referred to the fact that acts taken by one state which impact another only violate the principle of non-intervention where the former has 'a view to the coercion' of the latter: at 124 [241].

94 Delerue (n 15) 237.

95 Schmitt, 'The Law of Cyber Warfare' (n 24) 275.

96 See Silver (n 5) 83.

97 In the sense that they are not otherwise unlawful.

certain acts in response to internationally wrongful acts as countermeasures,[98] forceful countermeasures are likely prohibited by international law.[99] If non-kinetic cyber attacks were not considered forceful, states might see them as legitimate in response to wrongful acts which would permit recourse to countermeasures. In any event, they likely would be legally permitted as such. Thus, characterising cyber attacks as force prevents this countermeasure-based increase of their use and the escalation of harms that they may precipitate.

Further, the *jus cogens* status of the prohibition[100] in art 2(4) of the *UN Charter* excludes the possibility that states may rely on 'grounds precluding wrongfulness' as justifications for acts amounting to force.[101] If non-kinetic cyber attacks are not considered to be force, states may invoke these grounds as justification for such attacks, only further exacerbating their increased prevalence.[102] Such peremptory *jus cogens* norms also render void all treaties which conflict with their content,[103] and states are obligated to cooperate to bring to an end any unlawful breaches of these norms.[104]

2 *Armed Attack*

Plainly, the most pertinent ramification of including non-kinetic cyber attacks in the *jus ad bellum* as force under art 2(4) of the *UN Charter* is that they might amount to armed attacks under art 51 and enliven the right to self-defence in appropriate circumstances. As we will see, the precondition for forcible self-

---

98 *Responsibility of States for Internationally Wrongful Acts*, GA Res 56/83, UN GAOR, 56th sess, 83rd plen mtg, Agenda Item 162, Supp No 10, UN Doc A/RES/56/83 (28 January 2002, adopted 12 December 2001) annex ('*Responsibility of States for Internationally Wrongful Acts*') art 49(1); David J Bederman, 'Counterintuiting Countermeasures' (2002) 96(4) *American Journal of International Law* 817, 821; Enzo Cannizzaro, 'The Role of Proportionality in the Law of International Countermeasures' (2001) 12(5) *European Journal of International Law* 889, 893; Michael N Schmitt and Sean Watts, 'Collective Cyber Countermeasures?' (2021) 12(2) *Harvard National Security Journal* 373, 377; Nicholas Tsagourias, 'The Law Applicable to Countermeasures against Low-Intensity Cyber Operations' (2015) 14(1) *Baltic Yearbook of International Law Online* 105, 117.

99 *Delimitation of the Maritime Boundary (Guyana v Suriname) (Award)* (Permanent Court of Arbitration, Case No 2004–04, 17 September 2007) [446]; James Crawford, *State Responsibility: The General Part* (Cambridge University Press, 2013) 691; Olivier Corten, 'Judge Simma's Separate Opinion in the *Oil Platforms* Case: To What Extent Are Armed "Proportionate Defensive Measures" Admissible in Contemporary International Law?' in Ulrich Fastenrath et al (eds), *From Bilateralism to Community Interest: Essays in Honour of Bruno Simma* (Oxford University Press, 2011) 843, 849; Dev (n 4) 387; Ruys, 'The Meaning of Force' (n 62) 162; *Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/33 (n 98) art 50.

100 See above n 61.

101 *Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/33 (n 98) arts 26, 50. See also Ruys, 'The Meaning of Force' (n 62) 161.

102 Tom Ruys, 'The True Meaning of Force: A Reply to Mary Ellen O'Connell' (2014) 108 *American Journal of International Law Unbound* 148, 149.

103 *VCLT* (n 70) art 53; Stefan Kadelbach, 'Genesis, Function and Identification of *Jus Cogens* Norms' (2015) 46 *Netherlands Yearbook of International Law* 147, 162.

104 *Responsibility of States for Internationally Wrongful Acts*, UN Doc A/56/33 (n 99) arts 40 and 41.

defence is that a state suffers an "armed attack",[105] a subspecies of force.[106] If cyber attacks do not fall within the *jus ad bellum*, they cannot amount to armed attacks, at which point self-defence will not be permitted in response to their occurrence.[107] Conversely, if a cyber attack may amount to an armed attack, states may forcibly respond,[108] subject to customary restrictions of necessity and proportionality.[109] This might enable a state to 'hack back', utilise responsive cyber operations[110] or even where necessary to respond with kinetic means.[111] Given the significant ramifications even non-kinetic cyber attacks may have, this self-defence is crucial in protecting states' interests and safety.[112]

III "SCALE AND EFFECTS": A PHYSICAL BARRIER TO SELF-DEFENCE?

The notion that "unauthorised" force[113] is prohibited by the *UN Charter*, save for circumstances of self-defence, is at an abstract level settled.[114] Yet still 'grande confusion' has befallen *jus ad bellum* jurisprudence, and its practical application to novel circumstances remains shrouded in uncertainty, especially with the advent of technologies beyond the comprehension of those in the mid-20th century.[115] The aim of this Part is not to provide a full overview of the legal background — as much has been comprehensively dealt with elsewhere[116] — but to demonstrate

---

105 *UN Charter* (n 1) art 51.

106 *Nicaragua* (n 60) 101 [191]; Sean D Murphy, 'Terrorism and the Concept of Armed Attack in Article 51 of the UN Charter' (2002) 43(1) *Harvard International Law Journal* 41, 42–3; Constantine Antonopoulos, 'Force by Armed Groups as Armed Attack and the Broadening of Self-Defence' (2008) 55(2) *Netherlands International Law Review* 159, 160.

107 *UN Charter* (n 1) arts 2(4),51. See also Ruys, 'The Meaning of Force' (n 62) 163.

108 *UN Charter* (n 1) art 51.

109 *Nicaragua* (n 60) 103 [194]. See also Gray (n 58) 156; Tom J Farer, 'Drawing the Right Line' (1987) 81(1) *American Journal of International Law* 112, 113; Eaton (n 4) 761; Alison Pert, 'Proportionality in Self-Defence: Proportionate to What?' (2017) 24 *Pandora's Box* 65, 65.

110 Such as hacking into the systems of the aggressor to disrupt their operation or cause similar damage: Petkis (n 25) 1450.

111 *UN Charter* (n 1) art 51.

112 One potential qualm is that if cyber attacks may amount to force an aggressor might illegally use "forcible" cyber attacks below the "armed attack" threshold, yet victim states cannot forcibly respond in kind. To some extent this is true, however where the severity does not rise to an armed attack, traditional countermeasures likely suffice and prevent undue escalation of force.

113 A second exception to art 2(4) is that force may be "authorised" by the Security Council: *UN Charter* (n 1) arts 39, 41, 42.

114 Pert (n 109) 65; Iain Scobbie, 'Exceptions: Self-Defence as an Exception to the Prohibition on the Use of Force' in Lorand Bartels and Federica Paddeu (eds), *Exceptions in International Law* (Oxford University Press, 2020) 150, 171–2.

115 Tadashi Mori, *Origins of the Right of Self-Defence in International Law: From the Caroline Incident to the United Nations Charter*, tr Jonathan Bloch (Brill Nijhoff, 2018) 4; Richard A Falk, 'What Future for the UN Charter System of War Prevention?' (2003) 97(3) *American Journal of International Law* 590, 592; Elena Cirkovic, 'Incomplete World Order: United Nations Security Council Resolution 2249 (2015) and the Use of Force in International Law' (2016) 7(2) *Comparative Law Review* 1, 10.

116 See, eg, Gray (n 58) 120–99; Fu-Shun Lin, 'Self-Defence: A Permissible Use of Force under the UN Charter' (1963) 13(1) *DePaul Law Review* 43; Natalino Ronzitti, 'The Expanding Law of Self-Defence' (2006) 11(3) *Journal of Conflict and Security Law* 343; DW Greig, 'Self-Defence and the Security Council: What Does Article 51 Require?' (1991) 40(2) *International and Comparative Law Quarterly* 366; DW Bowett, *Self-Defense in International Law* (Manchester University Press, 1958); Ian Brownlie, 'The Use of Force in Self-Defense' (1961) 37 *British Yearbook of International Law* 183.

that physicality in nature or consequence is not an intrinsic component of "gravity" necessary to transform "mere" force into an "armed attack". Rather, notions of "armed attack" may encompass force which precipitates non-physical consequences of sufficiently grave "scale and effect".

A *Historical Interpretation of the UN Charter*

To demonstrate that "force" and "gravity" are not contingent on physical ramifications, it is prudent to ascertain what underlies this assumption and reveal that physical consequences have never been explicitly *required* to enliven rights to self-defence, even where such consequences have been *present* in previous cases.

1 *The Text of the UN Charter*

Whilst the *jus ad bellum* is grounded in both customary and treaty law,[117] it finds its most authoritative modern source in the *UN Charter*.[118] As alluded to, the relevant framework exists under arts 2(4) and 51 of the *UN Charter*.[119] Absent Security Council authorisation,[120] the right to use force exists only in self-defence under art 51: 'Nothing in the present *Charter* shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations'.[121]

Thus, questions of residual customary rights beyond the *UN Charter* aside,[122] it is generally accepted that the *conditio sine qua non* for forcible self-defence is that an 'armed attack' has occurred.[123] Once more, this concept remains undefined in the *UN Charter*. Taken in isolation, there is nothing textually to indicate that art 51 of the *UN Charter* only permits self-defence in response to armed attacks *with*

---

117 Huntley (n 18) 15.

118 Aiden Warren and Ingvild Bode, *Governing the Use-of-Force in International Relations* (Palgrave Macmillan, 2014) 9; John Norton Moore, '*Jus ad Bellum* before the International Court of Justice' (2012) 52(4) *Virginia Journal of International Law* 903, 910; Christopher R Rossi, '*Jus ad Bellum* in the Shadow of the 20th Century' (1994) 15(1) *New York Law School Journal of International and Comparative Law* 49, 60; Michał Kowalski, 'Some Remarks on the Relationship between the *Jus ad Bellum* Regulations under the UN Charter and Customary International Law: Why Does It Matter So Much?' (2018) 8(2) *Wroclaw Review of Law, Administration and Economics* 112, 113.

119 *UN Charter* (n 1) arts 2(4), 51.

120 Ibid arts 39, 41 42. See also Niels Blokker, 'Is the Authorization Authorized? Powers and Practice of the UN Security Council to Authorize the Use of Force by "Coalitions of the Able and Willing"' (2000) 11(3) *European Journal of International Law* 541, 544; Thomas M Franck, 'When, If Ever, May States Deploy Military Force without Prior Security Council Authorisation?' (2000) 4(2) *Singapore Journal of International and Comparative Law* 362, 362.

121 *UN Charter* (n 1) art 51.

122 See Ruys, *"Armed Attack" and Article 51* (n 63) 58.

123 Moore (n 118) 912; Rossi (n 118) 66; Judge Abdulqawi A Yusuf, 'The Notion of "Armed Attack" in the *Nicaragua* Judgment and Its Influence on Subsequent Case Law' (2012) 25(2) *Leiden Journal of International Law* 461, 462; Burkadze (n 7) 42.

physical consequences, especially if the argument that "force" need not be physical, as made by this article, is accepted.[124]

2 *The ICJ: Nicaragua and Beyond*

With the *UN Charter*'s text providing scant guidance, one may turn to how these provisions have been judicially interpreted. Despite art 51's foundational quality and *jus cogens* nature, uncertainty remains given the limited instances in which the ICJ has been called upon to adjudicate formal disputes about art 51 of the *UN Charter*.

The line of authority stems from the 1949 *Corfu Channel* case,[125] yet finds its most authoritative origins in the seminal 1986 *Military and Paramilitary Activities in and against Nicaragua* case ('*Nicaragua*').[126] In *Nicaragua*, the ICJ drew the formative distinction between 'armed attacks' and 'mere' uses of force.[127] This distinction was reliant on a so-called "gravity threshold", wherein 'the most grave forms of the use of force (those constituting an armed attack)' are distinguished from 'other less grave forms'.[128] The Court's only yardstick for this distinction was reference to the 'scale and effects' of the operation.[129] Here we are left to question the parameters of this phrase, for the Court neglected to describe its scope.[130] "Scale" has been generally accepted to refer to notions of extent, such as intensity, duration or geographical spread.[131] Meanwhile, "effects" has been taken to refer to the consequences.[132] Perhaps intentionally, although certainly for present purposes inconveniently, the Court did not elaborate on what form these consequences must take.[133] Importantly, there was nothing within the concept of "effects" which was explicitly tied to the *physical* consequences.

---

124 Even given the previous analysis of art 2(4) and its lack of an "armed" qualifier, there is nothing within the latter which indicates that any "arms" must approximate traditional military weaponry. Given the previously noted willingness of the ICJ to expand the provisions of the *UN Charter* to all forms of "weaponry", cyber weapons should not be excluded from art 51 on this ground. See also *Nicaragua* (n 61) 94 [176]; Preciado (n 29) 132.

125 *Corfu Channel (United Kingdom v Albania) (Merits)* [1949] ICJ Rep 4 ('*Corfu Channel*').

126 *Nicaragua* (n 60). See also Yusuf (n 123) 462; William Schabas, 'The Use of Force in the Nicaraguan Cases' in Edgardo Sobenes Obregon and Benjamin Samson (eds), *Nicaragua before the International Court of Justice* (Springer, 2018) 305, 305.

127 *Nicaragua* (n 61) 101 [191], 103–4 [195].

128 Ibid 101 [191].

129 Ibid 103–4 [195].

130 The Court did refer to a requirement that acts be so '[grave] as to amount to … [an] armed attack conducted by regular forces': ibid. This was, however, in the context of responsibility to clarify that if irregular forces sent by a state undertook acts which *if* conducted by military forces would amount to force, then such acts were not excluded from art 2(4). The Court therefore did not impose a *requirement* of conventional kinetic violence: ibid.

131 Georgina Redsell, 'Illegitimate, Unnecessary and Disproportionate: Israel's Use of Force in Lebanon' (2007) 3 *Cambridge Student Law Review* 70, 83; Tsagourias (n 18) 55.

132 Redsell (n 131) 73; Nicholas Tsagourias, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II' (2012) 15 *Yearbook of International Humanitarian Law* 19, 22.

133 Yusuf (n 123) 465; A Constantinou, 'Forcible Activities of Armed Bands as a Case of a Use of Force That Amounts to an Armed Attack in the Context of the Judgment of the ICJ in the Nicaragua Case' (1997) 9(1) *African Journal of International and Comparative Law* 156, 161; 何志鹏 [He Zhipeng] and 王惠茹 [Wang Huiru], «"非国家行为体" 对使用武力法的挑战与发展» [Challenges and Developments of the Law of Use of Force by "Non-State Actors"] (2019) 8 法学杂志［*Law Journal*] 44, 49 [tr author]; Buchan and Tsagourias (n 5) 123–4.

These principles have garnered ongoing approval in subsequent jurisprudence and, barring certain separate or dissenting judgments, have largely escaped judicial criticism therein.[134] In subsequent cases, the Court would not provide further exegesis of the meanings of "scale and effects" or "gravity".[135] Advisory opinions[136] offer little further guidance.[137] In all instances, the principles were cited without additional explanation, and in no case was the requirement of physicality considered, *let alone* decided upon.

It appears therefore that the position of the ICJ is essentially that outlined in *Nicaragua*: force will amount to an "armed attack" if its "scale and effects" are sufficiently "grave", whatever that term is deemed to entail. The same requirements must, in theory, apply to cyber attacks. The question then remains just how "scale and effects" applies to cyberspace.

B *Issues with the Lex Lata: "Virtually" Inapplicable?*

The youth of cyber warfare and lack of meaningful judicial engagement with arts 2(4) and 51 of the *UN Charter* since cyber attacks entered common practice is responsible for a dearth in directly applicable jurisprudence. Reversion to more generalist *jus ad bellum* principles does not satisfactorily translate to assessing cyber attacks. Such principles are, in their current form, irretrievably tied to kinetic warfare.[138] Thus, cyber attacks, which are able to cause significant harm even without physical consequences in a way which other uses of force may not, warrant bespoke consideration. By more closely analysing the legal landscape it is clear that notions of "gravity" as applied previously may appear inapplicable *because* they grappled with the physical realm, not that generalist *jus ad bellum* principles *must* be restricted to physical force.[139]

1 *The Jurisprudential Cyber Lacuna*

The point has already been laboured that the *UN Charter*, drafted in 1945, did not foresee the existence of cyber attacks.[140] The notion that harm equivalent to then-contemporary forms of force could be effected by non-kinetic means was alien. The result is a distinct lacuna in the international legal framework owing to the intrinsic difference between traditional kinetic attacks and non-kinetic cyber attacks. No case before the ICJ has addressed the application of the *jus ad bellum*

---

134 Yusuf (n 123) 465; Michał Kowalski, 'Original Sin Reaffirmed: The Nicaragua Judgement's Impact on the Notion of Armed Attack as the Most Grave Form of the Use of Force' (2016) 36 *Polish Yearbook of International Law* 37, 41–2. See, eg, *Oil Platforms (Islamic Republic of Iran v United States of America) (Judgment)* [2003] ICJ Rep 161, 187 [51] ('*Oil Platforms*'); *Armed Activities* (n 57); *Jus ad Bellum: Ethiopia's Claims 1–8 (Ethiopia v Eritrea) (Partial Award)* (2005) 26 RIAA 457, 466 [12] ('*Jus ad Bellum*'). See also Yusuf (n 124) 468; Roman Kwiecień, 'The Nicaragua Judgment and the Use of Force: 30 Years Later' (2016) 36 *Polish Yearbook of International Law* 21, 27.

135 *Oil Platforms* (n 134); *Jus ad Bellum* (n 134); *Armed Activities* (n 57).

136 See *Nuclear Weapons* (n 72); *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136.

137 Andrea Bianchi, 'Dismantling the Wall: The ICJ's Advisory Opinion and Its Likely Impact on International Law' (2004) 47 *German Yearbook of International Law* 343, 355.

138 Yusuf (n 123) 464; Dev (n 4) 390.

139 Petkis (n 25) 1447.

140 See above n 18.

to cyber attacks.[141] Whilst traditional warfare has been regulated by various treaty agreements, cyber warfare remains largely unregulated in a formal sense.[142] Perhaps the most authoritative source on the matter, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* ('*Tallinn Manual 2.0*') — whilst of significant informative value — is nonetheless an academic endeavour.[143] It also did not produce consensus amongst its experts on a number of critical issues including, pertinently, requirements of physicality for cyber armed attacks.[144] Simply, at present the manner in which the *jus ad bellum* applies to cyber attacks is undetermined. The lacuna in "settled" law, then, appears gaping.

2 *A Physical Gravity Threshold by Deduction?*

It is here that we encounter the central question of this section, querying whether anything in the principle underlying the nebulous "scale and effects" formulation requires physical manifestation, notwithstanding that no such requirement has been formally implemented to date. Consideration of the context of cases considered by the ICJ demonstrates that its decisions have determined the status of acts before it — in each case kinetic acts — but do not outline principles of universal applicability.[145] When *Nicaragua* was decided in 1986, cyberspace was in its infancy. The Court may only have had physical effects in mind, but that is not to say it endeavoured to formulate a principle to limit "force" thereto.[146] Judge Abdulqawi A Yusuf, former President of the ICJ, explicitly argues that in *Nicaragua* the Court was to characterise the acts before it, rather than to 'define an armed attack proper'.[147] Despite the march of time and technology, the fact remained that only kinetic acts were complained of to the ICJ, providing no opportunity for comment on cyber attacks or non-kinetic force generally. The ICJ thus developed, and subsequently relied upon, principles applicable in such kinetic situations. As Judge Yusuf would opine: '[w]hat this means is that the concept of "armed attack" in *Nicaragua*, and in the cases that were subsequently dealt with … is always contextually bound'.[148]

Noting the irrevocably differing context between traditional, physical and military force and cyber attacks, especially non-kinetic cyber attacks, these conceptualisations of gravity and "armed attack" must not be myopically taken outside of the context to which they are bound as if the cyber realm were analogous. With kinetic weapons, there is a clear correlation between gravity and physical effects.[149] Yet, in the 21st-century context and as applied to cyberspace, it is entirely conceivable that notions of "gravity" and "physicality" do not move in tandem so as to be broadly synonymous or correlative.[150] Insofar as not one

---

141 That is, the issue has not been raised directly in any relevant proceeding.
142 Nori Katagiri, 'Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks' (2021) 7(1) *Journal of Cybersecurity* 1, 2.
143 Schmitt, *Tallinn Manual 2.0* (n 20); Dev (n 4) 385.
144 Schmitt, *Tallinn Manual 2.0* (n 20) 342.
145 Yusuf (n 123) 465.
146 Petkis (n 25) 1447.
147 Yusuf (n 123) 465.
148 Ibid 462.
149 That is, the more serious the physical impact, the more "grave" the attack.
150 Boer (n 65) 15; Nguyen (n 4) 1122.

judgment dealing with art 51 of the *UN Charter* speaks of required *physical* gravity or *physical* effects, this requirement should not be inferred without further grounding. We cannot state blindly that physical effects are more grave than non-physical effects, or that the minimum intensity for an armed attack must lie somewhere above an intensity marked by physicality.

As noted in Part II, various examples of acts which would be considered potential armed attacks provided by the UN's *Definition of Aggression* bear no physical consequences.[151] As such, if one accepts that this demonstrates that physical *consequences* are not a component of aggression, one may derive the proposition that they should not be considered as required by "armed" force. Thus, the "armed" qualifier does not necessarily import a requirement of "physicality". By extension, an "armed" attack cannot, at least not solely by way of the "armed" qualifier, bear such a requirement. This demonstrates that it is possible that a physical *act* with non-physical consequences may suffice as an armed attack. We might now recall that cyber attacks which precipitate physical consequences, such as the explosion of a pipeline or meltdown of a nuclear reactor, would likely be considered armed attacks.[152] This consensus may ground a second proposition, being that an act itself need not be physical, or make use of traditional military weaponry, to have the potential to amount to an armed attack.

Taking these two propositions together, we see that for an "armed attack" in some instances there is not necessarily a requirement of physical *consequences*, and in others there is no requirement of a physical *act*. In sum, a non-kinetic cyber attack therefore ought not to be categorically excluded solely for lacking either of these clearly non-essential elements if its consequences are of sufficient gravity.

3 *Drafting of the "Armed Attack" Precondition*

With nothing at this juncture suggesting an "armed attack" *must* be physical, one might explore the intention of the drafters. Turning to the *travaux préparatoires* of the *UN Charter*,[153] the minutes of the United States Delegation to the San Francisco drafting conference provide an insight into the minutiae of drafting art 51. Therein it is shown that "armed attack" was inserted to replace the earlier term "aggression". However, upon deciding such a replacement was warranted, 'no substantial discussion took place as to its precise scope'.[154] This decision alone, often described with reference to the apparent obviousness of meaning to the drafters, is not sufficient to show that the intention was to *confine* the provision to physical affronts. Rather, in earlier drafts retaining the term 'aggression',

> [d]efinition was intentionally avoided … as it was impossible for a definition … to cover all instances of aggression … [and] attempting to define it would result in genuine acts of aggression being committed that did not fit the terms of the definition.[155]

---

151 See above nn 74–3.
152 See above n 23.
153 *VCLT* (n 70) art 32.
154 Ruys, *"Armed Attack" and Article 51* (n 63) 67.
155 Mori (n 115) 225.

Even when "armed attack" was substituted, a definition remained absent and nothing indicated that this hope to ensure that genuine affronts which warranted self-defence would not be excluded had abated. The intent of the drafters, it appears, was for the term to be left broad so as to be inclusive enough that "genuine acts" which would violate the intent of the provision yet were not foreseen or explicitly considered would not be excluded. As Tom Ruys notes, the intent was that any proposed acts to be included should be 'tested against present day [sic] customary practice'.[156] This implies that serious and harmful affronts such as non-kinetic cyber attacks would have been unlikely targets for exclusion by the drafters.

C *Indications from State Practice*

In discerning the possibility of non-physical armed attacks, examination of state perspectives towards cyber attacks specifically serves as an illustrative example. Such analysis may provide apt indication for the central proposition of this article, especially with the uncertainties arising from ICJ jurisprudence and the drafting of the *UN Charter*. However, it would be disingenuous to imply that state practice was entirely consistent and erroneous to depict it as fixed. It is also relatively non-existent in, ironically, practice, remaining instead largely as statements or policy positions.[157] Adding to the complexity is the fact that states continue to refine their stated positions. Nonetheless, exegesis of state practice does illuminate specific trends and elements of consistency that are informative.

The rapid developments in this area can be seen by the fact that writing only in 2018, relatively recently compared to the 1945 inception of the *UN Charter*, Christine Gray described that '[m]any states have now adopted cyber strategies, but these say only that international law is applicable'.[158] Since that time, several states — including Estonia,[159] France,[160] Germany,[161] Italy,[162] the Netherlands,[163]

---

156 Ruys, *"Armed Attack" and Article 51* (n 63) 68; *Iron Rhine Railway (Belgium v Netherlands) (Award)* (2005) 27 RIAA 35, 125 [79]–[81].

157 Buchan and Tsagourias (n 5) 116–17; Dev (n 4) 385.

158 Gray (n 58) 34.

159 *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established pursuant to General Assembly Resolution 73/266*, 76th sess, UN Doc A/76/136 (13 July 2021) 30 ('*UN Doc A/76/136*').

160 French Ministry of Defence, *International Law Applied to Operations in Cyberspace* (Position Paper, December 2021) 5.

161 German Federal Foreign Office, German Federal Ministry of Defence and German Federal Ministry of the Interior, Building and Community, *On the Application of International Law in Cyberspace* (Position Paper, March 2021) 15.

162 Ministry of Foreign Affairs and International Cooperation (Italy), Presidency of the Council of Ministers (Italy) and Ministry of Defence (Italy), *Italian Position Paper on 'International Law and Cyberspace'* (Position Paper, September 2021) 9.

163 Letter from the Minister of Foreign Affairs (Netherlands) to the President of the House of Representatives (Netherlands), 5 July 2019, 8 <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>, archived at <https://perma.cc/64SM-HMQZ> ('Netherlands Position').

New Zealand,[164] Norway,[165] Singapore,[166] Switzerland[167] and the United Kingdom[168] — have explicitly declared their view that cyber attacks may amount to force, armed attacks or both. As is clear from these declarations, there appears widespread acceptance that cyber attacks are forcible in nature and ought to be assessed by their "scale and effects", as with any other form of force. This, of course, is relevant insofar as the adoption and development of legal norms in this nebulous space will be tied to the acts and views of states. However, as within the literature, there is a divide even among those states which accept that cyber attacks may be forcible, centring around requirements of physicality.

Of the above, Estonia, the Netherlands, New Zealand, Norway, Singapore and Switzerland take a generalist approach, essentially claiming that if the "scale and effects" are sufficiently serious, the threshold will be met.[169] Others go further in disclaiming requirements of physicality. The US explicitly identifies major economic cyber attacks as potential armed attacks,[170] France notes 'a cyberoperation without physical effects may also be characterised as a use of force'[171] and the Netherlands 'cannot ... [rule] out that a cyber operation with very serious financial or economic impact may qualify as a use of force' or an armed attack.[172] This appears consistent with the perspective of the North Atlantic Treaty Organization, with Secretary-General Jens Stoltenberg claiming a 'serious cyberattack could trigger Article 5 of our founding treaty' and provoke collective self-defence.[173] In doing so, he cited the 2017 WannaCry ransomware attack, which 'shut down multiple hospitals and cost over £90 million'[174] but was not physical in effect.

Other states, however, such as Germany, Italy and the UK, claim that the "scale and effects" of cyber attacks must be "comparable" to conventional armed attacks, in many instances citing the *Tallinn Manual 2.0*.[175] Again, one is left to interpret the term "comparable", querying whether it speaks to nature or intensity. Interestingly, despite reference to equivalence with 'an armed attack using kinetic means', the UK also characterises a 'cyber attack which causes … severe economic or social consequences' as a 'Category 1 … [n]ational cyber

---

164 Ministry of Foreign Affairs and Trade (NZ) and Crown Law (NZ), *The Application of International Law to State Activity in Cyberspace* (Media Release, December 2020) 1.

165 *UN Doc A/76/136* (n 160) 69.

166 Ibid 84.

167 Federal Department of Foreign Affairs (Switzerland), *Switzerland's Position Paper on the Application of International Law in Cyberspace* (Position Paper, 27 May 2021) 4.

168 United Kingdom Mission to the United Nations, *Application of International Law to States' Conduct in Cyberspace* (Position Paper, 3 June 2021) 3.

169 See above nn 159–8.

170 Department of Defence (US), *Cyberspace Policy Report* (Report, November 2011) 3–4.

171 French Ministry of Defence (n 161) 3.

172 Netherlands Position (n 163) 4.

173 Jens Stoltenberg, 'NATO Will Defend Itself', *Prospect* (online, 27 August 2019) <https://www.prospectmagazine.co.uk/world/nato-will-defend-itself-summit-jens-stoltenberg-cybersecurity>, archived at <https://perma.cc/8C56-723W>.

174 Ibid; Sarah Chen and Jennifer Taw, 'Conventional Retaliation and Cyber Attacks' (2023) 8(1) *Cyber Defense Review* 67, 70; 'WannaCry Cyber-Attack Cost the NHS £92m after 19,000 Appointments Were Cancelled', *National Health Executive* (online, 12 October 2018) <https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled>, archived at <https://perma.cc/TQ35-SM65>.

175 See above nn 59, 162, 169.

emergency',[176] potentially supporting the contention that "comparable" has grown to refer more so to the latter.[177] This deduction would appear in line with the comments of Australia, which in a *Tallinn*-esque fashion outlined that whilst '[s]tates should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force',[178] this would involve not only considering physical impacts but also 'damage or destruction (including to their functioning) to objects or critical infrastructure'.[179] There is some blurring of distinctions here, yet reference to the "functioning" of critical infrastructure, even read alongside alternative considerations of damage, appears to demonstrate that physical effects are not required to be "comparable" to an attack involving traditional weaponry and thus an armed attack.[180]

A third group of states remains uncertain. China, for example, strongly argues that the prohibition on force applies to cyberspace.[181] However, it emphasises that understanding the precise details of applying the *jus ad bellum* to cyberspace must not be rushed and must be achieved by honest cooperation between states.[182] Russia similarly opines that 'the application of international law to the use of information and communications technologies … should not be automatic … [or] be carried out by simple extrapolation'.[183]

Thus, whilst state practice has largely adopted the notion of "scale and effects", there appears to exist discontent with the notion that gravity as applied to conventional warfare — that is, a *physical* gravity — should exclude non-kinetic attacks.[184] Whilst not universally agreed, an increasing number of states and international organisations appears to consider that in the appropriate circumstances non-kinetic cyber attacks can amount to armed attacks under art 51 of the *UN Charter* if their non-kinetic consequences are sufficiently "grave", including a number which had previously advocated for requirements of physicality.[185]

These statements are, however, merely stated position papers. As a result, their status as sources of international law remains subject to debate. Although they may

---

176 United Kingdom Mission to the United Nations (n 168) 3; National Cyber Security Centre (UK), 'Categorising UK Cyber Incidents' (online, 23 August 2023) <https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents>, archived at <https://perma.cc/UQY4-S9LL>.

177 Oorsprong, Ducheine and Pijpers (n 30) 225.

178 *UN Doc A/76/136* (n 159) 5.

179 Ibid.

180 Given Australia considers 'information technologies' as critical infrastructure: *Critical Infrastructure Resilience Report: Policy Statement* (Statement, 2015) 3 <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/Foreign_Investment_Review/Submissions>, archived at <https://perma.cc/9PLP-FPBY>.

181 张华 [Zhang Hua], «网络空间适用禁止使用武力原则的法律路径» [Legal Approaches to Apply the Prohibition of the Use of Force in Cyberspace], *安全内参* [*Internal Security*] (online, 29 March 2023) <https://www.secrss.com/articles/40792?fbclid=IwAR2Hpib1bYtGMxK0a6Yz7qIGpXUe7ACbiVWl83T6DjfLtkb4sOF-4NMjs9A> [tr author], archived at <https://perma.cc/9RL5-2S8L>.

182 Ibid.

183 *UN Doc A/76/136* (n 160) 80.

184 Buchan and Tsagourias (n 5) 122.

185 See, eg, nn 159–167.

reflect *opinio juris*, it is unclear whether they amount to formal state practice.[186] Nonetheless, they may be treated as indicating the opinions and approaches of states. Presently, as will be seen, their nature is such that they represent in writing the beliefs of states about the status of the law. Specifically, they deal with what will or will not amount to cyber force and cyber armed attacks. To that extent, they provide clarity on how states interpret the *lex lata* and demonstrate how they may act in practice. Absent any tangible acts amounting to practice, these positions provide the best indication of what may begin to form. To that extent, they may guide the creation of legal norms in this area, provide some form of certainty and, importantly, illustrate the legal views of states on an issue which still remains to be tested.

Therefore, despite not being formal acts of state practice, it is important that legal development, alongside strategic and policy development, accounts for these perspectives. As Michael N Schmitt notes, 'it is almost certain that states will begin to treat [non-kinetic] cyber operations as armed attacks',[187] and it is imperative that analytical frameworks reflect this burgeoning reality.

IV WHAT'S NEXT

With the legality of forcible self-defence in response to non-kinetic cyber attacks not adequately assessable by the contextually derived principles of the *jus ad bellum*, it has fallen largely to modern scholars to seek a solution. Importantly, they have often recognised that the *UN Charter* remains a 'living document' drafted to be adaptable to novel circumstances.[188] Such a jurisprudential approach is central to the *UN Charter*'s ongoing relevance some 80 years after its inception[189] and provides ample foundation for expansion to cyber attacks. In this Part, current scholarly frameworks for interpreting the *UN Charter* will be analysed to explicate that presently no solution is fit for purpose. This Part will then seek to provide such extension *de lege ferenda*, extrapolating a framework deemed the "Substantive Necessity" approach.

---

186 Jan Klabbers, 'The Redundancy of Soft Law' in Martti Koskenniemi (ed) *Sources of International Law* (Ashgate, 2000) 189, 190; Michael Akehurst, 'Custom as a Source of International Law' in Martti Koskenniemi (ed), *Sources of International Law* (Ashgate, 2000) 251, 251–3.

187 Schmitt (n 24) 283.

188 Thomas Franck, *Fairness in International Law and Institutions* (Oxford University Press, 1995) 260; Clark M Eichelberger, 'The United Nations Charter: A Growing Document' (1947) 252 *Annals of the American Academy of Political and Social Science* 97, 101; 'Secretary-General Presents His Annual Report to General Assembly' (Press Release No SG/SM/7136-GA9596, United Nations, 20 September 1999) <http://www.un.org/press/en/1999/19990920.sgsm7136.html>, archived at <https://perma.cc/NR83-PD7W>; Ove Bring, 'The Use of Force under the UN Charter: Modification and Reform through Practice or Consensus' in Jonas Ebbesson et al (eds), *International Law and Changing Perceptions of Security* (Brill Nijhoff, 2014) 1, 13; Jane E Stromseth, 'New Paradigms for the *Jus ad Bellum*?' (2006) 38(3) *George Washington International Law Review* 561, 563; James Larry Taulbee, 'Governing the Use of Force: Does the *UN Charter* Matter Anymore?' (2001) 4(2) *Civil Wars* 1, 8; Jessica Liang, 'Modifying the *UN Charter* through Subsequent Practice: Prospects for the Charter's Revitalisation' (2012) 81(1) *Nordic Journal of International Law* 1, 4; Ronald C Slye and Beth Van Schaack, *International Criminal Law: Essentials* (Aspen Publishers, 2009) 92; Łukasz Kulesa and Rafał Tarnogórski, 'The Future of the UN: Reinterpretation or Amendment of the UN Charter?' (2005) 5(2) *Polish Foreign Affairs Digest* 55, 62.

189 Eichelberger (n 189) 98. Cf Liang (n 189) 3.

A *Issues with Present Academic Approaches*

Whilst approaches proposed by scholars possess individual nuances and qualifications, secondary literature has widely found it apt to group these frameworks into three categories owing to their fundamental similarities, labelled 'instrument-based', 'target-based' and 'effects-based' approaches.[190] Ultimately, whilst each framework has its merits, each remains inappropriate for principled and pragmatic utilisation in the cyber realm.

1 *Instrument-Based*

Central to 'instrument-based' approaches is a focus on the weaponry employed. These approaches suggest a cyber attack may amount to an armed attack if it possesses sufficient intrinsic comparability to conventional weaponry or is employed to assist 'conventional' weapons.[191] Consequently, these approaches neglect analysis of outcomes or targets. Often it is argued that these approaches only capture instances where cyber attacks are a *component of*, or *prelude to*, physical attacks.[192] These approaches would likely include situations such as Russian cyber attacks on Viasat believed to target Ukrainian military communications a mere hour prior to Russia's invasion in February 2022, which assisted its conventional military force.[193]

Commonly levied criticisms of 'instrument-based' approaches depict them as 'outdated' or 'inflexible'.[194] Schmitt, for example, explicitly notes that such approaches are insufficient to address cyber attacks.[195] As noted, the analogy between the instruments of cyber attacks and traditional kinetic force is a strained one.[196] On one hand, a threshold only incorporating cyber technology with sufficient intrinsic comparability to traditional weaponry appears unlikely to capture the means most commonly used for such activities.[197] On the other hand,

---

190 Burkadze (n 7) 43; Spáčil (n 29) 29; Simmons (n 3) 53; Hathaway et al (n 3) 845; Nguyen (n 4) 1117; Delerue (n 15) 288.

191 Burkadze (n 7) 43; Hathaway et al (n 3) 845; Roscini, *Cyber Operations* (n 42) 50; Simmons (n 3) 54; Spáčil (n 29) 30; Nguyen (n 4) 1117.

192 Hathaway et al (n 3) 845–6.

193 'Russia behind Cyber Attack with Europe-Wide Impact an Hour before Ukraine Invasion', *National Cyber Security Centre* (Web Page, 10 May 2022) <https://www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion>, archived at <https://perma.cc/A288-TVZH>; Foreign, Commonwealth and Development Office (UK) and Elizabeth Truss, 'Russia behind Cyber-Attack with Europe-Wide Impact an Hour before Ukraine Invasion' (Press Release, 10 May 2022) <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>, archived at <https://perma.cc/X2XA-TNWM>; David E Sanger and Kate Conger, 'Russia Was behind Cyberattack in Run-Up to Ukraine War, Investigation Finds', *The New York Times* (online, 10 May 2022) <https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html>, archived at <https://perma.cc/RS9F-35DJ>.

194 Handler (n 8283) 227; Simmons (n 3) 55; Spáčil (n 29) 30; Nguyen (n 4) 1118.

195 Michael N Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts' in National Research Council, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (National Academies Press, 2010) 151, 163; Stephen Moore, 'Cyber Attacks and the Beginnings of an International Cyber Treaty' (2013) 39(1) *North Carolina Journal of International Law and Commercial Regulation* 223, 248; Burkadze (n 7) 43.

196 Buchan and Tsagourias (n 5) 118.

197 Delerue (n 15) 289; Burkadze (n 7) 43.

a threshold that considered computer technology per se as a sufficiently military instrument which would prima facie enliven a right to self-defence would be absurdly broad.

2 *Target-Based*

'Target-based' approaches evaluate attacks by virtue of that which they, as the name suggests, target.[198] The rhetoric largely centres on the supposed importance of the target, spoken in terms of 'sufficiently important … system[s]'[199] or 'critical infrastructure'.[200] Overt questions of material damage are foreign.[201]

A purely 'target-based' approach is unacceptably broad.[202] If one considers solely what is targeted, one neglects the success or likelihood of success of the operation and is blind to the potential practical ramifications of an attack *of that kind* on the target.[203] Further, a state may deem any target sufficiently important that an attack on it will justify responsive force. For example, the US has deemed 'nearly all government or commercial activit[ies]' sufficiently important targets.[204] Consequently, responsive force is permitted in an extensive range of scenarios which otherwise might not warrant self-defence. Such a broad approach unnecessarily heightens the risk of conflict in practice.[205]

3 *Effects-Based*

Under 'effects-based' approaches, primacy is given to the consequences as opposed to the characteristics of the act itself.[206] Whilst there exists significant variance within this school of thought, for most, if the 'scale and effects' of the consequences of a cyber attack are sufficiently grave, the right to self-defence will be enlivened.[207] Oftentimes, the approach proposed by Schmitt[208] and noted by the authors of the *Tallinn Manual 2.0*[209] is considered the leading version of the framework.[210] Schmitt's approach incorporated the six criteria of (i) severity, (ii) immediacy, (iii) directness, (iv) invasiveness, (v) measurability and (vi) presumptive legitimacy.[211] The literature largely concurs that 'effects-based'

---

198 Nguyen (n 4) 1119; Burkadze (n 7) 43; Simmons (n 3) 56; Delerue (n 15) 288; Hathaway et al (n 3) 846.

199 Moore (n 195) 247; Hathaway et al (n 3) 846; Burkadze (n 7) 43; Spáčil (n 29) 30.

200 Sharp (n 20) 130; Spáčil (n 29) 30; Simmons (n 3) 56; Delerue (n 15) 288.

201 Sharp (n 20) 130; Spáčil (n 29) 30.

202 Hathaway et al (n 3) 846–7; Delerue (n 15) 288; Simmons (n 3) 57.

203 Delerue (n 15) 288; Roscini (n 42) 54; Spáčil (n 29) 31; Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Brill Nijhoff, 2015) 138.

204 Simmons (n 3) 57; Nguyen (n 4) 1121; Preciado (n 29) 121.

205 Spáčil (n 28) 31.

206 Huntley (n 18) 25; Burkadze (n 7) 43; Simmons (n 3) 58.

207 Schmitt, *Tallinn Manual 2.0* (n 20) 331; Simmons (n 3) 58; Eaton (n 4) 698; Spáčil (n 29) 36; Chen and Taw (n 174) 69.

208 Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37(3) *Columbia Journal of Transnational Law* 885, 914–15 ('Computer Network Attack').

209 The *Tallinn Manual 2.0* (n 20) adopts Schmitt's criteria, but with the addition of the criteria '[m]ilitary character' and '[s]tate involvement' and the substitution of the criterion "presumptive legitimacy" with '[p]resumptive legality': at 333–7.

210 Nguyen (n 4) 1122; Spáčil (n 29) 31.

211 Schmitt, 'Computer Network Attack' (n 208) 914–15.

approaches receive the most support from scholars and states alike.[212] Despite this status, effects-based approaches are not above criticism. This article does not, however, seek to entirely discredit such approaches but rather to demonstrate not-insignificant shortcomings which must be addressed.

The effects-based frameworks as understood unfairly prejudice non-kinetic cyber attacks by importing requirements of physicality.[213] As outlined, this threshold is not grounded in jurisprudence or policy but in history and ought not to be myopically transposed into the cyber context. Whilst some scholars accept that a sufficiently severe non-physical attack would suffice, this appears a distinctly minority view; to most scholars, the effect must be physical.[214] This understanding continues to neglect the fact that the harm caused by cyber attacks will necessarily differ in nature yet not necessarily in seriousness and that an inability to respond in self-defence where required could be devastating. The notion of comparability relied upon by scholars such as Schmitt is often a literal one, meaning that, as Katharine C Hinkle notes, 'this approach is as notable for what it leaves out of the "armed attacks" category as [for] what it brings into it'.[215] Effects-based frameworks are also inherently consequentialist, meaning that states must wait until the consequences of an attack have manifested *with sufficient seriousness* before they can take preventative forceful action.[216] This problem is only exacerbated by the rapidly developing nature of cyber attacks, whose tangible effects may not be able to be confirmed for a significant time or due to a lack of technology.[217]

Whilst Schmitt's factors may be of use in analysing an attack, comprehensive and accurate use of this complex multivariate model in fast-paced crisis situations appears untenable[218] given the need for a quick response to any attack.[219] Further shortcomings are apparent in that often the standard required for effects or severity may be unclear or inherently subjective.[220] Effects-based frameworks have repeatedly been faced with the critique that in providing 'criteria' in the form of descriptors alone their application is at the behest of the state and that often, when applied to cyber attacks, they may give rise to diametrically opposed conclusions depending on the aims or emphasis of the user.[221] For example, whilst Schmitt applied his factors to demonstrate that the Estonian DDoS attacks were armed attacks,[222] Reese Nguyen was able to persuasively apply them to demonstrate that

---

212 Delerue (n 15) 288; Simmons (n 3) 58; Hathaway et al (n 3) 847; Spáčil (n 29) 31.

213 Petkis (n 25) 1448.

214 Shaun Roberts, 'Cyber Wars: Applying Conventional Laws to War to Cyber Warfare and Non-State Actors' (2014) 41(3) *Northern Kentucky Law Review* 535, 555.

215 Katharine C Hinkle, 'Countermeasures in the Cyber Context: One More Thing to Worry About' (2011) 37 *Yale Journal of International Law Online* 11, 11.

216 See, eg, Schmitt, *Tallinn Manual 2.0* (n 20) 914–15.

217 Petkis (n 25) 1448.

218 Dev (n 4) 391.

219 Pantaleone Nespoli et al, 'Optimal Countermeasures Selection against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks' (2018) 20(2) *Institute of Electrical and Electronics Engineers Communications Surveys and Tutorials* 1361, 1363.

220 Spáčil (n 29) 31.

221 Nguyen (n 4) 1124; Simmons (n 3) 61.

222 Schmitt, 'Cyber Operations' (n 27) 577.

they were not.[223] Notions such as "severity" are inherently 'malleable':[224] either the attacks *were* severe as they crippled cyber systems[225] or they *were not* because nobody was injured.[226] No doubt states in practice would err on the side of the former to expand rights to self-defence.

B *A Novel Framework: Substantive Necessity*

We have now seen that in the context of cyber attacks extant paradigms for assessing self-defence must be replaced with an approach that is more nuanced and aligned with state practice. As cyber attacks continue to intensify on the global stage, such a task is no doubt pressing.[227] Yet at the same time, cautionary considerations must not be forgotten. After all, a key principle underpinning the *UN Charter* is to *prevent* forceful acts where possible rather than to encourage them.[228] With this in mind, the field is, for all intents and purposes, clear to propose such a solution. To the extent that proposals to amend the *UN Charter* to account for cyber attacks would almost certainly fail[229] and given the eminent foreseeability that a treaty-based approach would not find adequate support, a novel framework operating within the present *UN Charter* structure is necessary.

Recognising the exigencies and vicissitudes facing any novel framework, this article proposes a multifaceted standard capable of wide and flexible application termed the "Substantive Necessity" approach. This approach, it is argued, allows states to assess when a cyber attack has sufficiently grave consequences so as to allow the use of forcible self-defence under art 51 of the *UN Charter*, even if these consequences are non-physical. Under the Substantive Necessity approach, a cyber attack will amount to an "armed attack" animating the legal right to forcible self-defence where it is *apprehended by the victim state based on clear and convincing evidence as a hostile act or set of acts which (a) has fundamentally compromised, or (b) is imminently poised to fundamentally compromise, the (i) functioning or (ii) security of (c) infrastructure crucial to a state's ability to function as such.*

---

223 Nguyen (n 4) 1123–4.

224 Ibid 1123; Simmons (n 3) 61–2.

225 Schmitt, 'Cyber Operations' (n 27) 577.

226 Nguyen (n 4) 1123–4.

227 Harjinder Singh Lallie et al, 'Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic' (2021) 105 *Computers and Security* 102248:1–20, 3; Shannon Williams, 'Number of Cyberattacks Will Continue to Increase in 2023', *SecurityBrief Australia* (online, 11 January 2023) <https://securitybrief.com.au/story/number-of-cyberattacks-will-continue-to-increase-in-2023>, archived at <https://perma.cc/4YUF-5E83>; Joy LePree Anderson, 'Global Cyberattacks Increased 38% in 2022', *Security* (online, 20 January 2023) <https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022>, archived at <https://perma.cc/69HB-4H7Y>; Brad Ryan, 'Microsoft to Help Australia Build "Cyber Shield", Anthony Albanese Announces in Washington', *ABC News* (online, 24 October 2023) <https://www.abc.net.au/news/2023-10-24/anthony-albanese-in-washington-dc-microsoft-deal/103012802>, archived at <https://perma.cc/3KPV-3AFA>.

228 *UN Charter* (n 1) Preamble.

229 Liang (n 188) 4; Shirley V Scott, 'The Question of UN Charter Amendment, 1945–1965: Appeasing "the Peoples"' (2007) 9(1) *Journal of the History of International Law* 83, 88; Carolyn L Willson, 'Changing the Charter: The United Nations Prepares for the Twenty-First Century' (1996) 90(1) *American Journal of International Law* 115, 125; Karen A Mingst and Margaret P Karns, *The United Nations in the 21st Century* (Westview Press, 4th ed, 2012) 50.

It is readily observable that this framework borrows elements of existing approaches. Such appropriation is not unintentional but recognises the meritorious components of each approach and supplements them with additional considerations to mitigate their shortcomings.

1 *Apprehended by the Victim State Based on Clear and Convincing Evidence*

The Substantive Necessity approach's condition precedent requires that the state targeted by a cyber attack apprehend the criteria enlivening legal rights to self-defence[230] "based on clear and convincing evidence". Notably, this inclusion of what appears to be an evidentiary standard is not necessarily reflective of the legal obligations owed by the state acting in self-defence but rather provides a practical guideline in formulating a decision to respond.

Perhaps subtly, the fact that "apprehension" must be on the part of the "victim state" improves equitable application. States no doubt possess differing cyber capabilities.[231] Oftentimes, the most vulnerable states possess worse technology than those attacking them.[232] By requiring an apprehension of the *victim state*, the Substantive Necessity approach ensures that the burdens of apprehension are not placed above the legitimate technological capacity of a state being targeted. In any event, whilst the approach makes this explicit, it is almost unavoidable that subjective apprehension will be employed by states in practice.[233]

Far from imposing an arbitrary standard ripe for exploitation, the potentially subjective "apprehension" is fettered by requirements of "clear and convincing evidence". This standard is not foreign to use-of-force jurisprudence[234] and adequately places a robust threshold restricting force and requiring that states consider the grounds for their supposed apprehension. It must be acknowledged that international law 'does not currently have a well-developed body of evidentiary rules on the use of force' nor 'any straightforward, express statement of the standard of proof expected'.[235] However, there are 'indications in international law that the standard should be something like the clear and

---

230 The element of "apprehended by the victim state" reflects the fact that the Substantive Necessity approach, being a framework which is applied to determine whether forcible self-defence is permissible in response to a cyber attack, is applied by the state subject to that cyber attack.

231 Daniele Archibugi, Mario Denni and Andrea Filippetti, 'The Technological Capabilities of Nations: The State of the Art of Synthetic Indicators' (2009) 76(7) *Technological Forecasting and Social Change* 917, 925; Martin Bell and Keith Pavitt, 'The Development of Technological Capabilities' in Irfan ul Haque et al (eds), *Trade, Technology, and International Competitiveness* (World Bank, 1995) 69, 70–1.

232 Lech J Janczewski, 'An Overview of the Unique ICT Situation of Small States' in Lech J Janczewski and William Caelli (eds), *Cyber Conflicts and Small States* (Routledge, 2016) 33, 44; Yuchong Li and Qinghui Liu, 'A Comprehensive Review Study of Cyber-Attacks and Cyber Security: Emerging Trends and Recent Developments' (2021) 7 *Energy Reports* 8176, 8179–80; Christopher Darby and Sarah Sewall, 'The Innovation Wars: America's Eroding Technological Advantage' (2021) 100(2) *Foreign Affairs* 142, 142.

233 After all, a state would not neglect to act in self-defence on mere speculation that more advanced technology might have precipitated a different conclusion.

234 Mary Ellen O'Connell, 'Rules of Evidence for the Use of Force in International Law's New Era' (2006) 100 *American Society of International Law Proceedings* 44, 45.

235 Ibid 44. See also Alejandro Chehtman, 'The Use of Force' in Carlos Espósito and Kate Parlett (eds), *The Cambridge Companion to the International Court of Justice* (Cambridge University Press, 2023) 448, 454; Ruys, *"Armed Attack" and Article 51* (n 63) 546.

convincing standard found in the United States'.[236] In cases concerning art 51 of the *UN Charter* it appears that whilst evidence beyond reasonable doubt has not been required, more than cursory evidence has been.[237]

The "clear and compelling" standard, situated between the two aforementioned alternatives, appears to garner support from various international tribunals[238] and in the literature.[239] Because an objective grounding is required, states are precluded from claiming a mere subjective belief to receive legal exculpation for using force. This is congruent with the restrictive aims of the *jus ad bellum* and ensures that forcible self-defence is only permitted in response to an armed attack 'which is clear, unambiguous, subject to proof, and not easily open to misinterpretation or fabrication'.[240]

By including such phraseology, the Substantive Necessity approach provides a clear guide to states as to what is expected of them. Even if this approach is not applied in a legalistic sense by states during conflict, the question of whether the basis of a state's desire to act in self-defence is "clear and compelling" may be readily answered in the lay sense. This provides an important guardrail against states seeking forceful recourse, even if imperfectly applied as a practical, rather than legal, standard.

2 *Hostile Act or Set of Acts*

The Substantive Necessity approach is also specific about the quality of the affront captured, being acts — individual or cumulative — accompanied by a hostile intent.

Importing a requirement of hostility aligns the Substantive Necessity approach with general state practice on forcible self-defence. History is replete with examples of states claiming to have suffered an armed attack or to be legally justified in responsive force with reference to the intent of the perpetrator.[241] This requirement is referred to, albeit not extensively, in *Nicaragua* where the ICJ noted that owing to a lack of information on 'possible motivations' it was 'difficult to decide' if an armed attack had occurred.[242]

In practice, the requirement acknowledges that a cyber attack that requires self-defence will likely be hostile, meaning force will be required to end the intentional affront. Intrusion into cyber systems or causing harm thereto without hostile intent

---

236 O'Connell (n 234) 45.

237 See, eg, *Oil Platforms* (n 134) 195 [71]*; Nicaragua* (n 60) 85–6 [159].

238 *Trail Smelter (United States of America v Canada) (Award)* (1938/1941) 3 RIAA 1905, 1964; *Velásquez Rodríguez v Honduras (Merits)* (Inter-American Court of Human Rights, Series C No 4, 29 July 1988) [127] ('*Velásquez Rodríguez*').

239 Dinah L Shelton, 'Judicial Review of State Action by International Courts' (1989) 12(3) *Fordham International Law Journal* 361, 386; Christopher J Greenwood, 'International Law and the United States' Air Operation against Libya' (1987) 89(4) *West Virginia Law Review* 933, 935; Jules Lobel, 'The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan' (1999) 24(2) *Yale Journal of International Law* 537, 547.

240 Louis Henkin, 'The United Nations and Its Supporters: A Self-Examination' (1963) 78(4) Political Science Quarterly 504, 532.

241 Ruys, *"Armed Attack" and Article 51* (n 63) 172.

242 *Nicaragua* (n 60) 120 [231].

is likely only if the attack spread by mistake or missed its intended target.[243] Whilst severe damage may result from such a mistake, there appears little utility in allowing an attack which would only be retaliatory, especially if the mistake cannot be rectified. If the perpetrating state is unable to stop the attack, then a forceful response will do nothing but escalate conflict and damage. More appropriate remedies, such as reparations, would suffice. If the perpetrating state was able to stop the attack but decided not to, then it is argued that such a decision would transform the act into one of hostile intent, thus enlivening the right to self-defence.

Furthermore, by requiring the cyber attack be an "act" in the sense understood by international law,[244] the approach ensures that only actively undertaken conduct of the requisite nature will permit self-defence, with no scope to claim that a failure or an omission to act suffices.[245] This again is aimed at restricting the unnecessary escalation of force and prevents the imposition of additional duties of protection on other states in respect of cyber force that are not present in respect of physical force. It is important to clarify here the distinction between an omission to act and an omission to rectify as described above. Under the approach, a state would not be liable to recourse if it simply failed to actively intervene to stop acts of another state in which it had no involvement. Such omissions fall outside the approach. However, as outlined, the perpetrating state's omission to rectify its own act should, under the Substantive Necessity approach, be considered with reference to the act itself. The harm precipitated continues on from the initial act rather than the omission. Thus, the perpetrating state's wilful decision to not stop that act creates a constructive intent, rendering it responsible for the harms that flow from that act. This remains the case even where the initial act was not intended to cause harm. At the point at which knowledge of the harm arises, and the state declines to cease its act, a constructive intent is formed.

The Substantive Necessity approach also expressly adopts the 'Nadelstichtaktik', or 'accumulation of events theory', reflecting the fact that an accumulation of smaller-scale acts, taken together, may permit self-defence even

---

243 See, eg, Daniel E Capano, 'Throwback Attack: How NotPetya Ransomware Took Down Maersk', *Industrial Cybersecurity Pulse* (online, 30 September 2021) <https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/>, archived at <https://perma.cc/4G4R-BDUT>. See also Matteo Iaiani et al, 'Analysis of Cybersecurity-Related Incidents in the Process Industry' (2021) 209 *Reliability Engineering and System Safety* 107485:1–20, 7; Neil C Rowe, 'Ethics of Cyber War Attacks' in Lech J Janczewski and Andrew M Colarik, *Cyber Warfare and Cyber Terrorism* (Information Science Reference, 2008) 105, 108.

244 See, eg, *Velásquez Rodríguez* (n 238) [170].

245 Franck Latty, 'Actions and Omissions' in James Crawford, Alain Pellet and Simon Olleson (eds), *The Law of International Responsibility* (Oxford University Press, 2010) 355, 356; Gordon A Christenson, 'Attributing Acts of Omission to the State' (1991) 12(2) *Michigan Journal of International Law* 312, 321; John C Hall, 'Acts and Omissions' (1989) 39(157) *Philosophical Quarterly* 399, 405–6.

where each individual act may not suffice.[246] This recognises that ultimately the harm, whether it is caused by one act or many distinct acts, will ultimately have the same impact.[247] It may be the case that a single cyber act is either indistinguishable or itself unable to satisfy the approach, but that many taken in conjunction as part of a concerted attack should nonetheless be deemed sufficient where pragmatically prudent. After all, it would be illogical as discussed previously for seriously harmful cyber campaigns to fall outside the *jus ad bellum* on technicalities if they may otherwise be captured. The holistic treatment of potentially distinct cyber attacks, especially where they may be perpetrated cumulatively by a large number of individual operators on behalf of states rather than by one source, is therefore crucial.

Such a framework was also endorsed by the *Tallinn Manual 2.0* as appropriate for cyber attacks[248] and indeed would appear in line with the stated positions of states.[249] Moreover, this framework expressly emphasises the gravity of an attack in substance rather than mere form, allowing for the normative imperatives of the Substantive Necessity approach to not be undermined by a technicality that an overall cyber campaign might consist of distinct acts that cause cumulative devastation.

3 *Fundamentally Compromised or Is Imminently Poised*

Whilst lamenting existing emphases on physicality, we have nonetheless seen the imperatives underpinning a requirement of severity that raises "mere" force to an "armed attack". The first way the Substantive Necessity approach incorporates this threshold is through a requirement reminiscent of, yet more clearly defined than, Schmitt's 'severity',[250] being to "fundamentally compromise". This distinguishes the approach from overly broad target-based frameworks and reduces the potential for exploitation present in existing effects-based frameworks. It does, however, draw on the useful elements present in effects-based frameworks to attempt to categorically and clearly outline when non-kinetic cyber attacks will possess sufficient "scale and effects" to amount to armed attacks.

There is inherent to many "critical infrastructure" approaches the view that an affront that merely "disrupts" or "interferes with" the function of a target that the

---

246 Such an approach was alluded to in *Nicaragua* (n 60) 109–10 [231], *Oil Platforms* (n 134) 191–2 [64] and *Armed Activities* (n 57) 222–3 [146]. The literature also broadly appears to accept this theory: Ruys, *"Armed Attack" and Article 51* (n 63) 174; Albrecht Randelzhofer and Georg Nolte, 'Article 51' in Bruno Simma et al (eds), *The Charter of the United Nations: A Commentary* (Oxford University Press, 3rd ed, 2012) vol 2, 1397, 1409; Delerue (n 15) 334–5; Terry D Gill and Paul AL Ducheine, 'Anticipatory Self-Defense in the Cyber Context' (2013) 43 *Israel Yearbook on Human Rights* 81, 106; Mark B Baker, 'Terrorism and the Inherent Right of Self-Defense (A Call to Amend Article 51 of the United Nations Charter)' (1987) 10(1) *Houston Journal of International Law* 25, 42; Victor Kattan, 'Israel, Hezbollah and the Conflict in Lebanon: An Act of Aggression or Self-Defense?' (2006) 14(1) *Human Rights Brief* 26, 27.

247 Mark R Jacobson, 'War in the Information Age: International Law, Self-Defense, and the Problem of "Non-Armed" Attacks' (1998) 21(3) *Journal of Strategic Studies* 1, 13; Boris Kondoch, 'North Korea and the Use of Force in International Law' (2013) 18(2) *Korean Journal of Security Affairs* 4, 14.

248 Schmitt, *Tallinn Manual 2.0* (n 20) 342.

249 See above nn 159–168.

250 Schmitt, *Tallinn Manual 2.0* (n 20) 333–7.

state has deemed especially "critical" will enliven the right of self-defence.[251] Whilst such a low threshold may be satisfactory in seeking to characterise whether a specific act amounts to force, this article argues that when considering whether an act amounts to an "armed attack" this view is too permissive. Noting the imperatives of restricting recourse to force, it is unacceptable to consider even minor affronts as armed attacks that would permit self-defence even if the target is important. Conversely, to "fundamentally compromise" carries connotations of severity.[252] It implies something more than inhibition or frustration that may be persevered through, even with increased difficulty.[253] The impact is *fundamental* to the nature of the target; it has been so *compromised* as to prevent reliance. To "fundamentally compromise" also presents a minimum threshold of severity beyond which the right of self-defence would be enlivened. This also appears to be in line with state practice, as outlined previously, which has largely accepted that there must be a genuinely severe interference with specific targets for force to become an armed attack.[254] The requirement under the Substantive Necessity approach incorporates these positions but defines them more clearly than the nebulous terminology employed by states. This article argues that this is appropriate both in terms of reflecting the will of states and also in practice in terms of setting the "gravity" threshold.

Acknowledging concerns for the retrospectivity of effects-based frameworks,[255] this enquiry provides for an assessment to be made both reasonably ex ante and ex post facto. Even where the target is yet to be fundamentally compromised — and thus yet to see the significant harms precipitate — in circumstances where it is (apprehended on clear and convincing evidence as) imminently poised to do so, self-defence may be warranted. By requiring that states apprehend not that an attack *has* had a certain effect, but that it is *imminently poised* to have said effect, the Substantive Necessity approach ensures that a state need not wait until the initial attack has played itself out. As a result, cyber attacks may be promptly responded to and their most devastating consequences potentially prevented.

This notion is not itself novel, nor does it provide untrammelled license to consider an attack as "imminent". Rather, it invokes the doctrine of 'anticipatory self-defence' as understood in customary international law.[256] Stemming from the

---

251 Ibid 282–3; Boer (n 65) 25; Delerue (n 15) 304.

252 *Oxford English Dictionary* (online at 15 August 2024) 'fundamentally' (def 1); *Oxford English Dictionary* (online at 15 August 2024) 'fundamental' (def 1).

253 'Compromise', *Computer Security Resource Center* (Web Page) <https://csrc.nist.gov/glossary/term/compromise>, archived at <https://perma.cc/963C-A5XR>.

254 See above the discussion regarding states which have adopted the "scale and effects" approach.

255 Petkis (n 25) 1448.

256 The precise status of the doctrine is not settled, with the ICJ 'express[ing] no view': *Nicaragua* (n 60) 103 [194]. See also Matthew C Waxman, 'The Caroline Affair in the Evolving International Law of Self-Defence', *Lawfare* (online, 28 August 2018) 2 <https://scholarship.law.columbia.edu/faculty_scholarship/2507>, archived at <https://perma.cc/H5Y3-YVUS>; Ezdi (n 230) 33; Schmitt, 'The Law of Cyber Warfare' (n 24) 285.

seminal Caroline affair,[257] the proposition of US Secretary of State Daniel Webster speaking of a 'necessity of self-defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation'[258] is often invoked as justifying proportionate self-defence against an 'imminent' threat.[259] The doctrine itself remains controversial, and is not universally accepted by academics or states,[260] owing largely to textual interpretation of the retrospective language of art 51 of the *UN Charter*.[261] Nonetheless, there exists a significant school of thought that supports the existence of the doctrine, often citing the "inherent right" to self-defence posited by art 51 of the *UN Charter* and the purported customary law surrounding anticipatory self-defence.[262] Moreover, whilst the ICJ has neglected to make findings on the issue, as Samantha Ria Shahriar describes at length, state practice appears to indicate 'deeply entrenched' beliefs as to rights of anticipatory self-defence.[263] Indeed, even if practice were mixed on this issue, the fact that cyber attacks may be essentially instantaneous once they have been fully operationalised may undermine any capacity for retrospective response and may cause potentially devastating harms renders it irrational to prevent states from responding, in appropriate circumstances, where an attack is apprehended until the effects have manifested and it is effectively "too late". Therefore, even if anticipatory self-defence is not appropriate in the context of traditional military force, it should be considered as appropriate in the context of cyber attacks because of their unique nature.

The Substantive Necessity approach makes as much explicit in its formulation and is governed appropriately by the same strictures as would govern the customary anticipatory self-defence doctrine in kinetic contexts.[264] It is also careful to note that it is not sufficient that a state apprehend that an attack might

---

257 See Howard Jones, 'The Caroline Affair' (1976) 38(3) *The Historian* 485; Nguyen Van Sang, 'The Caroline Affair and the Diplomatic Crisis between Great Britain and the United States, 1837–1841' (2018) 8 *Prawo i Polityka* [Law and Politics] 73.

258 Letter from Daniel Webster to Lord Alexander Baring Ashburton, 27 July 1842 <https://lccn.loc.gov/09022080>, archived at <https://perma.cc/FM4E-N3D9>.

259 James A Green, 'Docking the *Caroline*: Understanding the Relevance of the Formula in Contemporary Customary International Law concerning Self-Defense' (2006) 14(2) *Cardozo Journal of International and Comparative Law* 429, 464; Gábor Kajtár, 'The Caroline as the "Joker" of the Law of Self-Defence: A Ghost Ship's Message for the 21st Century' (2018) 21(1) *Austrian Review of International and European Law* 3, 3; James A Green, 'The *Ratione Temporis* Elements of Self-Defence' (2015) 2(1) *Journal on the Use of Force and International Law* 97, 104; Ezdi (n 230) 32.

260 Samantha Ria Shahriar, 'The Issue of Imminence: Can the Threat of a Cyber-Attack Invoke the Right to Anticipatory Self-Defence under International Law?' (2020) 9 *UCL Journal of Law and Jurisprudence* 55, 57.

261 Ibid 69.

262 Ibid; John Alan Cohan, 'The Bush Doctrine and the Emerging Norm of Anticipatory Self-Defense in Customary International Law' (2003) 15(2) *Pace International Law Review* 283, 322–8.

263 Reference is made by Shahriar to UN reports, the Third Arab-Israeli War, the US campaigns in Libya and Afghanistan, speeches of prominent UK government officials, the actions of the UN Security Council and other UN documents: Shahriar (n 260) 70–1.

264 David Kretzmer, 'The Inherent Right to Self-Defence and Proportionality in *Jus ad Bellum*' (2013) 24(1) *European Journal of International Law* 235, 250; Chris O'Meara, *Necessity and Proportionality and the Right of Self-Defence in International Law* (Oxford University Press, 2021) 11; Chris O'Meara, 'Reconceptualising the Right of Self-Defence against "Imminent" Armed Attacks' (2022) 9(2) *Journal on the Use of Force in International Law* 278, 280.

occur in the future or, indeed, the near future. Rather, a specific attack must itself be imminently poised to take effect in the requisite manner.

This also increases the deterrence factor of the Substantive Necessity approach. If a state had to wait for manifest consequences before being able to respond, its ability to respond might be significantly inhibited. This means that, for aggressor states, the risk of engaging in a cyber attack might be considered worthwhile. However, if a cyber attack may be responded to before it has had the desired effect, or even in circumstances where it is unclear that it will succeed overall, then the risk is significantly heightened.

4 *Functioning or Security*

It is not sufficient that any component of the requisite infrastructure is fundamentally compromised. Rather, an attack must undermine the "functioning or security" of the infrastructure as a whole. This standard limits forceful recourse to situations of severe necessity and attacks of sufficient gravity and once again crystallises the standard at which the "scale and effects" of an attack are severe enough so as to warrant recourse by force rather than other means.

To fundamentally compromise "functioning", an attack must prevent infrastructure from working or operating for its intended purpose.[265] For example, a power grid shutdown would prevent the power grid from fulfilling its purpose of delivering electricity to citizens. It is not enough that a component of the infrastructure's function is prevented from working or that its functioning is moderately inhibited; rather, the compromise must be *fundamental* to the infrastructure itself. The fact that the power grid would produce electricity at a lower rate than before would impact its function but would not fundamentally compromise it. The fact that a nuclear plant might not be able to communicate with the outside world might fundamentally compromise its ability to communicate but not its function of generating power. Thus, again, the severity of the non-kinetic effects is grounded specifically and at a level of sufficient centrality to the targeted infrastructure.

Alternatively, to fundamentally compromise "security", it must be that the infrastructure is no longer protected adequately against external control or further exploitation.[266] As an illustration, if malware were introduced which allowed an external cyber operator to control or direct a military weapons system, the security of that infrastructure would be lost. The malware would become such a serious threat, which may itself cause significant harm or could be used so as to enable future significant harms, that it could be defended against with force. For example, the 2020 SolarWinds hack involved hackers, supposedly backed by a state, gaining access to computer networks and systems through a backdoor and being able to

---

265 *Oxford English Dictionary* (online at 15 August 2024) 'functioning' (def 1); *Oxford English Dictionary* (online at 15 August 2024) 'function' (def 1).

266 Trent Jaeger, *Operating System Security* (Springer, 2008) 3–4; *Oxford English Dictionary* (online at 15 August 2024) 'security' (def 1); 'Glossary', *Australian Government Department of Home Affairs* (Web Page) <https://www.protectivesecurity.gov.au/resources/glossary>, archived at <https://perma.cc/ZRQ3-WGHJ>.

upload malware to tens of thousands of devices.[267] Again, mere incursions or minor exploitations would be insufficient, as the security must be *fundamentally* compromised. A hacker gaining the mere ability to listen to intercepted communications would not fundamentally compromise the security of a military institution, whereas a hacker gaining the ability to remotely control the nuclear weapons of a state would.

Plainly, owing to the central importance of the "functioning or security" of infrastructure which is itself "crucial", an attack on such a target would be of sufficient "gravity" to warrant forcible self-defence. Again, here the fact that the Substantive Necessity approach considers that attacks which undermine the "functioning or security" of the relevant infrastructure is sufficiently grave to enliven the right of self-defence does not mean that it claims that such attacks chart the metes and bounds of "gravity" in the cyber context. Rather, it argues that specific instances of suck attacks will be sufficiently grave in their "scale and effects". It is readily foreseeable that, with advances in technology and cyber attacks, further examples with different consequences may nonetheless be so grave as to be armed attacks enlivening the right of self-defence.

5 *Infrastructure Crucial to a State's Ability to Function as Such*

There is nothing particularly novel about the notion of "critical infrastructure" in the cyber attack literature.[268] In any event, its inclusion here is narrowed further to "infrastructure crucial to the ability for a state to function *as such*", that is, as a state. This caveat narrows the scope of targets to targets attacks on which *necessitate* response through force, unlike impermissibly broad target-based or "critical infrastructure" approaches.[269]

As discussed previously, presently what constitutes "critical infrastructure" is often left to the determination of individual states.[270] Whilst there appear to be some consistent features in domestic definitions — such as requirements that

---

267 Saheed Oladimeji and Sean Michael Kerner, 'SolarWinds Hack Explained: Everything You Need to Know', *TechTarget* (online, 3 November 2023) <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know>, archived at <https://perma.cc/T3F8-DDS3>.

268 See, eg, C Gallais and E Filol, 'Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure' (2017) 16(1) *Journal of Information Warfare* 64; Buchan and Tsagourias (n 5); Hodgkinson (n 7); Kilovaty (n 3); Oorsprong, Ducheine, and Pijpers (n 30); Simmons (n 3); Schmitt, 'The Law of Cyber Warfare' (n 24) 284; Preciado (n 29) 101.

269 Boer (n 65) 25.

270 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, GA Res 58/199, UN GAOR, 58th sess, Agenda Item 91(b), UN Doc A/RES/58/199 (30 January 2004, adopted 23 December 2003); SC Res 2341, 7882nd mtg, UN Doc S/RES/2341 (13 February 2017) 2. See also Colleen M Newbill, 'Defining Critical Infrastructure for a Global Application' (2019) 26(2) *Indiana Journal of Global Legal Studies* 761, 764; Roberto Setola, Eric Luiijf and Marianthi Theocharidou, 'Critical Infrastructures, Protection and Resilience' in Roberto Setola et al (eds), *Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach* (Springer, 2016) 1, 2–3; Christer Pursiainen, 'The Challenges for European Critical Infrastructure Protection' (2009) 31(6) *Journal of European Integration* 721, 722; Jakub Harašta, 'Legally Critical: Defining Critical Infrastructure in an Interconnected World' (2018) 21 *International Journal of Critical Infrastructure Protection* 47, 48.

infrastructure be vital, necessary or essential to national functions or safety[271] — it is also the case that states adopt additional broad considerations such as "wellbeing" or "government function".[272] It is not unforeseeable that emphasis placed by individual states on certain aspects of society would inform definitions of "critical infrastructure". States can apply self-serving definitions to this nebulous term, and as seen with examples — such as that of the US — described previously, it is likely that states will err on the side of inclusion and expansion of their own rights to self-defence.

The Substantive Necessity approach directly addresses this problem. It does so by defining "critical infrastructure" more concretely, thereby limiting states' discretion to define it more expansively. Infrastructure must be crucial, or *required*, for the functioning of the state *as such*. This formulation speaks to the inherent operations, duties and characteristics that define a state and enable it to exist, operate and be recognised as a manifestation of the determination of its people. These include, but are not limited to, what is required for ensuring the safety of citizens, facilitating the economy, maintaining military defence and providing *essential* public services. Infrastructure of convenience or utility will not suffice. Examples such as public transport networks, whilst important, are not crucial to the existence of the state *as such*, even where they might otherwise be deemed "critical infrastructure". Conversely, the central banking systems of a state, especially in an increasingly digitalised economy, dictate the function of the state *as such* through its economy and are therefore captured under this definition.

Nevertheless, characterisation of infrastructure as "crucial to a state's ability to function" does require careful consideration to ensure that "crucial" is not interpreted too expansively. Some regimes may very well perceive infrastructure beneficial to the government's power, such as propaganda apparatuses, as fundamental to their function, or seek to expand the definition to infrastructure which *facilitates* the effective function of the state.

The definition of "critical infrastructure" under the Substantive Necessity approach, however, has two safeguards against this. First, the distinct reference to the *state* rather than the *government* places the emphasis on the body politic rather than the ruling powers.[273] In much the same way that civil war might be viewed

---

271 See, eg, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001*, Pub L No 107-56, § 1016(e), 115 Stat 272; *Security of Critical Infrastructure Act 2018* (Cth) s 30BEA; 'Critical National Infrastructure', *National Protective Security Agency (UK)* (Web Page, 25 April 2023) <https://www.npsa.gov.uk/critical-national-infrastructure-0>, archived <https://perma.cc/X66M-7LGG>; Federal Ministry of the Interior (Germany), *National Strategy for Critical Infrastructure Protection* (Report, 17 June 2009) 4.

272 See, eg, «关键信息基础设施安全保护条例» [Regulations on the Security Protection of Critical Information Infrastructure] (People's Republic of China) State Council, Order No 745, 30 July 2021, art 2; Information Security Policy Council (Japan), *Second Action Plan of Information Security Measures for Critical Infrastructures* (Report, 3 February 2009) 10.

273 Theresa Paola Stawski, 'The State-Regime-Nexus: Law and Legal Order' (2021) 15(3) *Zeitschrift für Vergleichende Politikwissenschaft* [Journal for Comparative Politics] 357, 360; Dino Bozonelos et al, *Introduction to Comparative Government and Politics* (Academic Senate for California Community Colleges, 2022) 70; Robert M Fishman, 'Rethinking State and Regime: Southern Europe's Transition to Democracy' (1990) 42(3) *World Politics* 422, 427; Kevin Ward, 'Regime', *Encyclopaedia Britannica* (Web Page, 21 January 2016) <https://www.britannica.com/topic/regime>, archived at <https://perma.cc/5TTN-YL89>.

as an expression of a *state*'s self-determination[274] or that a state may continue to function despite changing governments or systems of government, this does not permit the inclusion of regime-centric factors. Second, the requirement that infrastructure be "crucial" almost amounts to a "but for" test. Infrastructure can only be "crucial" if the state is unable to operate as such absent the infrastructure. Mere considerations of ease or efficiency will not suffice.

C *Robustness Testing the New Approach*

Whilst the above analysis explains factors and scenarios which permit self-defence where appropriate, when push comes to (cyber) shove the Substantive Necessity approach should be framed robustly so that "generous" interpretation by states is not so expansive as to undermine its effectiveness but also so that states have legal recourse to self-defence where necessary. To test the veracity of the approach, this section will explore whether acts commonly understood as non-kinetic and harmful to states, yet not warranting forceful recourse, would be appropriately excluded[275] and whether those which ought to be considered sufficiently grave would be included.

1 *Appropriately Exclusive*

(a) Disinformation or Electoral Interference

Drawing particular notoriety in recent times has been the use of cyber means to allegedly spread disinformation or propaganda, especially with the intent of influencing another state's internal political processes, such as its elections, perhaps epitomised to many by the alleged Russian campaign to interfere with the

---

274 Wouter G Werner, 'Self-Determination and Civil War' (2001) 6(2) *Journal of Conflict and Security Law* 171, 175; Kathleen Gallagher Cunningham, *Inside the Politics of Self-Determination* (Oxford University Press, 2014) 40; Kyle Beardsley, David E Cunningham and Peter B White, 'Resolving Civil Wars before They Start: The UN Security Council and Conflict Prevention in Self-Determination Disputes' (2017) 47(3) *British Journal of Political Science* 675, 676; Solomon E Salako, 'Civil Wars and the Right to Self-Determination' (2013) 2(1) *International Law Research* 129, 140.

275 Noting previous distinctions with economic coercion, such acts are plainly not captured.

2016 US presidential election.[276] Such acts venture plainly into the domain of a violation of the principle of non-intervention yet are widely accepted as not amounting to an "armed attack".[277] Whilst there exists potential for disruption or political harm through such means, and the impact on a state may be significant, they do not necessitate armed responses. Misinformation may be responded to domestically — for example, through media or communication — and indeed forceful recourse against an external state is unlikely to remedy the damage caused internally within the political system.[278]

Such acts, whilst able to be met with countermeasures,[279] fall outside the scope of the proposed approach. Whilst they might interfere with or disrupt political processes, they do not *fundamentally compromise* the processes they are directed at. Even if the electoral process was considered a sufficient target, the function of that process would continue insofar as citizens could make a free decision, even if based on erroneous grounds. The increased provision of such erroneous grounds does not mean the function is unable to occur as intended from a mechanism standpoint. At its highest, the effectiveness or efficiency of the function is impeded. The act would be appropriately excluded.

(b) Espionage

With governments now storing sensitive information digitally within computer networks, such data has emerged as both crucial and a significant risk. Information impacting national security or the functions of the state remains a valuable target

---

276 See generally Joe Burton, 'Cyber-Attacks against the UK Electoral Commission Reveal an Ongoing Threat to Democracy', *The Conversation* (online, 16 August 2023) <https://theconversation.com/cyber-attacks-against-the-uk-electoral-commission-reveal-an-ongoing-threat-to-democracy-211550>, archived at <https://perma.cc/ZPT7-BYEZ>; Kimberly Lim, 'Singapore Presidential Election: Authorities Warn against Foreign Interference, "Malicious" Cyber Threats', *South China Morning Post* (online, 15 August 2023) <https://www.scmp.com/week-asia/politics/article/3231176/singapore-presidential-election-authorities-warn-against-foreign-interference-malicious-cyber>, archived at <https://perma.cc/AUB6-9H3F>; Ayanna Alexander, 'Security Experts Warn of Foreign Cyber Threat to 2024 Voting', *Associated Press* (online, 22 February 2023) <https://apnews.com/article/iran-united-states-government-russia-arizona-3cbfa1c46051416fac1f4183774a0f05>, archived at <https://perma.cc/8867-DNJ6>; Simon Benson, 'Don't Mess With Our Democracy, Home Affairs Minister Clare O'Neil Warns', *The Australian* (online, 21 February 2023) <https://www.theaustralian.com.au/nation/dont-mess-with-our-democracy-home-affairs-minister-clare-oneil-tells-china/news-story/d1cfea70b676c72708b73f8e4012b07f>, archived at <https://perma.cc/56EV-67MV>; Will Ziebell, 'Australia Forms Task Force to Guard Elections from Cyber Attacks', *Reuters* (online, 9 June 2018) <https://www.reuters.com/article/us-australia-security-elections-idUSKCN1J506D>, archived at <https://perma.cc/NLW9-PP9S>; 'Canada Opens Inquiry into Allegations of Election Meddling by China, Russia', *Al Jazeera* (online, 7 September 2023) <https://www.aljazeera.com/news/2023/9/7/canada-opens-inquiry-into-allegations-of-election-meddling-by-china-russia>, archived at <https://perma.cc/PH6Z-6CKJ>.

277 Alex Xiao, 'Responding to Election Meddling in the Cyberspace: An International Law Case Study on the Russian Interference in the 2016 Presidential Election' (2020) 30(2) *Duke Journal of Comparative and International Law* 349, 358; Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination, and the Principle of Non-Intervention in Cyberspace' in Dennis Broeders and Bibi van den Berg (eds), *Governing Cyberspace: Behavior, Power, and Diplomacy* (Rowman & Littlefield, 2020) 45, 51.

278 Muhammad Faizal Bin Abdul Rahman et al, *Countermeasures against Foreign Interference* (Report, April 2020) 16–19; Xiao (n 277) 377.

279 Xiao (n 277) 361; Michael N Schmitt, 'Foreign Cyber Interference in Elections' (2021) 97 *International Law Studies* 739, 762; Rahman et al (n 278) 12.

of espionage from hostile states.[280] The theft thereof, despite potential seriousness, does not amount to a use of force.[281] Since this is a covert intelligence-gathering exercise which does not harm or coerce directly and is carried out almost ubiquitously by states,[282] permitting forceful recourse would be disproportionate and could lead to widespread escalation.[283]

Such activities are no doubt not captured by most of the Substantive Necessity approach. The only requirement which might give pause is that of the "security" of infrastructure. However, this argument may be dismissed. The security referred to is of the infrastructure itself rather than the data contained therein per se. If espionage rose to such a level that there was a fundamental compromising of the systems, such as a cyber incursion allowing for ongoing control over key systems, then this would have ramifications which could amount to an armed attack. However, it is this newfound cyber influence rather than the espionage per se which *might* enliven a right to self-defence. No doubt this is rightly so. Mere cyber espionage would not be caught by the Substantive Necessity approach unless its extent went further and took on a different fundamental nature as described so as to no longer be espionage. Thus, espionage remains appropriately excluded.

2 *Appropriately Inclusive*

(a) Major Economic Shutdown

The characterisation of major economic devastation as permitting self-defence is rife with conflict in the literature.[284] Indeed, it is perhaps *the* example upon which schisms rotate. After all, it is significantly impactful yet distinctly not physical. This article has been clear that the ramifications are sufficiently impactful to citizen and state that they ought to enliven a right to self-defence both as a recourse and as a deterrence.

Attacks which cause such major economic damage — such as devastating banking systems, stock markets or financial systems generally — would no doubt be captured. It is unclear how a state is to function, as a state, without its economy. The infrastructure that permits the existence and use of money where the world has moved away from cash and where wealth is substantially tied up intangibly is crucial to the function of a society and its economy. To that extent, a cyber attack which caused a major economic shutdown would fundamentally compromise the function of infrastructure crucial to the state's function as such and would be captured.

---

280 Dominik Herrman, 'Cyber Espionage and Cyber Defence' in Christian Reuter (ed), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (Springer Vieweg, 2019) 83, 84; William C Banks, 'Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage' (2017) 66(3) *Emory Law Journal* 513, 515; Jon R Lindsay, 'Cyber Espionage' in Paul Cornish (ed), *The Oxford Handbook of Cyber Security* (Oxford University Press, 2021) 223, 225.

281 Preciado (n 29) 135; Petkis (n 25) 1447.

282 Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' (2012) 20(2) *CommLaw Conspectus: Journal of Communications Law and Policy* 363, 364; Joe Devanny, Ciaran Martin and Tim Stevens, 'On the Strategic Consequences of Digital Espionage' (2021) 6(3) *Journal of Cyber Policy* 429, 431; Banks (n 280) 513.

283 Devanny, Martin and Stevens (n 282) 430; Jarno Limnéll, 'Proportional Response to Cyberattacks' (2017) 1(2) *Cyber, Intelligence, and Security* 37, 51.

284 See, eg, Buchan and Tsagourias (n 5) 120–1.

Interestingly, this also demonstrates the nuance present in the approach. The example has been posited in this article of the destruction of a single stock exchange building. Application of the approach to such an occurrence becomes contingent on the actual effect of the attack. A cyber attack which shuts down a single trading location in a large, intertwined economy may cause economic harm but might otherwise not affect the economy. Stock prices may drop and trades from that location may be unable to occur, but the effect is not fundamental. No doubt under the approach taken by this article such an attack would amount to a use of force, but it would not enliven the armed attack threshold. Conversely, if the attack targets a number of exchanges, or a more fundamental economic institution, such that the economy or financial system is severely impacted, then the standard would be enlivened as described and the attack appropriately included. Importantly, this demonstrates the necessity for a bespoke approach here to art 51 of the *UN Charter*. Under present conceptions of force and armed attack, it is possible that the lack of physical consequences as a result of such economic impacts would mean that such an attack would not be considered as force or an armed attack. This is normatively and legally undesirable and further demonstrates the usefulness of the present standard.

(b) Attacks with Other Significant Non-Physical Ramifications

Intuitively, there are a number of scenarios that may be contemplated whose ramifications may be non-physical in their *direct* effect yet simultaneously sufficiently dangerous or serious that they both enliven the right to self-defence and require the concomitant deterrence to aggressor states which the exercise of this right brings.

Such scenarios may be explored through indicative, but non-exhaustive, examples. Cyber attacks which cripple an electricity grid in a modern society may do so by interfering with the systems underpinning the infrastructure yet may plunge civilisations into darkness, halt essential services or communications, disrupt livelihoods and ultimately put lives at risk. Similarly, cyber attacks which impact healthcare infrastructure directly, undermine emergency communication systems or destroy other essential utilities may have devastating impacts and must be prevented. As attacks on such infrastructure may in some instances impact physical safety, these are captured. Finally, cyber attacks which substantially inhibit military infrastructure — as a prelude to physical attack or otherwise — would strike at a fundamental area of statehood, being the defence force and its capacity to defend the nation, and would be captured.

V CONCLUSION

In an era where states exhibit ever-increasing reliance on the digital realm,[285] it is plainly unsatisfactory that they cannot defend against attacks on digital systems as they may against attacks on physical assets or infrastructure, including where necessary with force. This proposition and the need to maintain the aims of the *UN Charter*, particularly the prohibition of force, are not mutually exclusive.[286]

---

[285] See above nn 3 and 4.

[286] Simmons (n 3) 87; Hathaway et al (n 3) 849.

The *UN Charter* was not drafted to apply for the handful of decades following its inception only to require renegotiation when circumstances or technologies changed. The foundational document of modern international relations is by all accounts a "living document" and ought to be interpreted with flexibility to enable its continued application. Yet to date, present approaches to interpreting arts 2(4) and 51 of the *UN Charter* with respect to cyber attacks inadequately account for the nuances of cyberspace. Such approaches are not comfortably concomitant with the realist approaches of states in practice and therefore are unlikely to be accepted as legitimate. This anachronism is only exacerbated in situations where the "gravity" criterion is considered through the lens of notions of physicality which were derived in contexts well before non-physical attacks of the ilk of cyber attacks were possible. The critical question is, therefore, just how the *UN Charter* shall apply to the lacuna resulting from the underlying differences between cyber attacks and traditional kinetic warfare.

In answering this pressing query, this article has argued that a novel and principled approach to interpreting the *UN Charter* is required with due deference to the context and nature of acts undertaken state-against-state. It has argued that gravity, being a criterion of severity not of physicality, may still exist in the cyber realm. It has therefore argued that a cyber attack should be considered as amounting to an "armed attack" animating the legal right to forcible self-defence where it is *apprehended by the victim state based on clear and convincing evidence as a hostile act or set of acts which (a) has fundamentally compromised, or (b) is imminently poised to fundamentally compromise, the (i) functioning or (ii) security of (c) infrastructure crucial to a state's ability to function as such*. This approach appropriately empowers states to defend themselves where necessary whilst preventing the "opening of the floodgates" of force in international relations.

Conflict continues to evolve. One need only look to Russia's 'concerted [cyber] campaign to disrupt Ukrainian critical infrastructure'[287] in its 'Special Military Operation' or the US' frequent use of drones in the Middle East[288] to see that as states develop new technologies, they also find ways to use these technologies to exert force in new ways. It is imperative that such hostile acts be regulated and deterred by international law. The solution may be readily envisaged: the *UN Charter* must be interpreted to appropriately account for hostile acts in the cyber realm. Perhaps then, when we may perceive with greater certainty that these harmful acts no longer occupy their legal lacuna but are bound by the *jus cogens* illegality of force and enliven the protective ambit of self-defence, we might better declare *per jus ad bellum processimus*, *et in jus contra bellum evolvimus*.[289]

---

287 Marcus Willett, 'The Cyber Dimension of the Russia-Ukraine War' (2022) 64(5) *Global Politics and Strategy* 7, 7; Seonghwan Choi, 'Analysis and Aspects of Space Warfare in the Russia-Ukraine War (Russian Invasion of Ukraine) and Considerations for Space Technology Development' (2022) 2(2) *Journal of Space Technology and Applications* 169, 170; Paul Ducheine, Peter Pijpers and Kraesten Arnold, 'Bits- or Blitzkrieg? Cyber Operations in the Russia-Ukraine War' (2022) 46(3) *Atlantisch Perspectief* [Atlantic Perspective] 42, 44.

288 Leila Hudson, Colin S Owens and Matt Flannes, 'Drone Warfare: Blowback from the New American Way of War' (2011) 18(3) *Middle East Policy* 122, 123; Christine Sixta Rinehart, *Drones and Targeted Killing in the Middle East and Africa: An Appraisal of American Counterterrorism Policies* (Lexington Books, 2016) 23.

289 'Through the right to war we have proceeded, and into the law against war we have evolved'.