# Regulating the Use and Conduct of Cyber Operations through International Law: Challenges and Fact-finding Body Proposal

Jiang Zhifeng*

**ABSTRACT**

*Although cyber operations present an emerging threat to international peace and security, there is a lack of interstate agreement on the international regulation of cyber operations. One prevailing response is to theoretically extend existing international law to the cyber domain. This paper, however, challenges this existing response. It argues that international law is theoretically limited in regulating the use and conduct of cyber operations. With regards to use, there are limits to prohibiting cyber operations as internationally wrongful acts of a state. Three internationally wrongful acts are examined. These are prohibited "use of force", as well as violations of the non-intervention and self-determination principles. With respect to conduct, there are limits to constraining the destructive effects of cyber operations through International Humanitarian Law (IHL). The character of cyber warfare and the nature of societies in which cyber warfare is conducted pose unique challenges to the applicability and effectiveness of IHL provisions. In order to address the limitations faced by international law in regulating the use and conduct of cyber operations, this paper concludes by proposing an independent fact-finding body.*

* LLB (NUS), BA (Yale-NUS). The author would like to thank Assistant Professor Rohan Mukherjee for his guidance and insightful comments, as well as Adjunct Associate Professor Gérardine Goh Escolar for her helpful feedback. Any errors and omissions remain the author's own. The author can be contacted at jiangzhifeng@u.yale-nus.edu.sg.

## INTRODUCTION

The threat of mutually assured destruction posed by nuclear weapons has constrained and deterred the blatant use of conventional weapons in interstate disputes between major powers. Cyber operations thus offer an attractive strategic alternative of imposing costs on states while avoiding full-blown conventional warfare. For this reason, cyber operations are also particularly attractive tools in asymmetric conflicts. Cyber operations refer to the "employment of cyber capabilities to achieve objectives in or through cyberspace."[1] Such objectives include physical damage, as well as economic and political disruption. This paper will analyse two types of cyber operations: Those used to inflict physical damage such as civilian causalities and infrastructural damage and those that inflict non-physical damage, namely economic and political disruption.

The capacity to cause damage both within and outside of cyberspace has led to the characterization of cyberspace as the fifth domain of war. In contrast to the air, land, sea, and space domains of warfare, cyberspace is arguably more anarchical due to the current dearth of international laws governing cyberspace. Regulatory responses to cyber operations conducted within and through cyberspace have largely revolved around the use of national laws. National laws are insufficient. This is because the cyber domain faces a security dilemma, a situation where "the means by which a state tries to increase its security decrease the security of others."[2] A state's efforts to increase its cyber security through the creation of more sophisticated cyber defensive and offensive weapons can cause states to *subjectively* feel vulnerable, thereby leading to continuous build-up of cyber weaponry. This is attributable to how states "act in terms of the vulnerability they feel, which can differ from the actual situation"[3] and that "states are uncertain about their adversaries' motives, lacking confidence that others are pure security seekers".[4] This security dilemma faced by states is more acute in cyberspace. Cyber operations are offense-dominant, in that they are strategically advantageous, financially cheaper, and technically easier to attack first than to

[1] Michael N Schmitt, *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations* (Cambridge University Press 2017) 564.
[2] Robert Jervis, 'Cooperation Under The Security Dilemma' (1978) 30 World Politics 169.
[3] ibid 174.
[4] Charles L Glaser, 'The Security Dilemma Revisited' (1997) 50 World Politics 195.

defend against an attack. This is because "an attacker has to be successful only once, whereas the defender has to be successful all of the time", especially where modern society is a "target-rich environment" due to heavy reliance on cyber technology.[5]

Furthermore, the effectiveness of an offensive cyber operation is transient, in that it is contingent on the continuing existence of the vulnerability in the cyber system. The longer a state withholds an attack, the greater the likelihood that the vulnerability will be identified and patched. Furthermore, first strike cyber operations can limit and even neutralize the ability of the victim state to launch both conventional and cyber retaliatory attacks.[6] Such advantages associated with offensive cyber operations increase incentives for first strikes. This is not true of nuclear weapons and conventional weapons in a world where mutually assured destruction and second strike capabilities have negated the advantages of offensive attacks vis-à-vis defense.

This paper aims to contribute to existing legal scholarship in two ways. First, this paper contends that existing international law is inadequate in regulating the use and conduct of cyber operations. With respect to the legality of using cyber operations, there are fundamental limits to classifying cyber operations as internationally wrongful acts. With respect to regulating the conduct of cyber operations, cyber operations challenge the effectiveness of international humanitarian law (IHL) in limiting civilian causalities in situations of armed conflict. Second, with respect to addressing regulatory gaps in the cyber domain, this paper challenges the existing focus on an international cyber treaty. By integrating law and political science perspectives, this paper instead proposes an independent fact-finding body without prosecutorial or enforcement capabilities as a possible regulatory measure for the cyber domain.

[5] John Sheldon, 'Deciphering Cyberpower: Strategic Purpose in Peace and War' (2011) 5 Strategic Studies Quarterly 98.
[6] Ilai Saltzman, 'Cyber Posturing and the Offense-Defense Balance' (2013) 34 Contemporary Security Policy 44. See also Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Manoeuvre, and Manipulate in the Digital Age* (Public Affairs 2016) 12.

## I. CYBER OPERATIONS AS INTERNATIONALLY WRONGFUL ACTS

While cyber operations that inflict substantial physical damage *may* be illegal, cyber operations that cause non-physical damage are not outlawed under international law. For a cyber operation to be considered an internationally wrongful act of a state, it must (a) be attributable to the state under international law, and (b) constitute a breach of an international obligation of the state.[7]

### The problem of attribution

First and foremost, before a cyber operation can be legally attributable to a state, it must be possible to identify the actor behind the operation. The "prior process of tracing material proof of the identity of the perpetrator" is required before entering the next stage of whether the act can be legally imputed to the state.[8] Identification of specific cyber warfare actors, however, may be complicated by the deliberate use false-flag operations, IP address masking, and identity 'spoofs' to obstruct identification. Nevertheless, the identification of cyber operations is not impossible but is instead a matter of degree in terms of accuracy and speed.[9]

Assuming that the perpetrators behind cyber operations are identified, for the state to be internationally responsible for a cyber operation, the operation has to be attributable to the state under international law. The nature of cyber operations poses serious challenges to finding attribution. Given the clandestine and loose relationship between state and the non-state actors, it is improbable for cyber operations to meet the high thresholds of attribution under Articles 4 and 5 of the 2001 ILC Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), which reflect customary international law.[10] Article 4

[7] International Law Commission (ILC) 'Elements of an internationally wrongful act of a State, Responsibility of States for Internationally Wrongful Acts' (2001) Article 2.
[8] *Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v United States of America)* [1986] ICJ [57].
[9] Joseph S Nye, 'Deterrence And Dissuasion In Cyberspace' (2017) 41 International Security 51.
[10] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, [2007] ICJ [401].

requires the actor to function as an organ of a state by exercising legislative, executive, or judicial functions. Article 5 requires the actor to exercise elements of governmental authority, in that the internal law of the state has authorized the actor to exercise public functions.[11] Unlike conventional warfare, where the armies of two states engage in armed conflicts, cyber operations intricately involve non-state actors, such as politically or financially-driven lone hackers or informal groups of hackers, as well as private entities such as private military and security corporations.[12] Using non-state proxies or outsourcing cyber warfare operations to private corporations to conduct cyber warfare can allow states to strategically distance themselves from cyber operations through plausible deniability.

The other two attribution tests would be the effective control test laid out in *Nicaragua* and *Bosnia Genocide* and the overall control test stipulated by *Tadic*.[13] The thresholds of these tests are, however, not easily met. Under the effective control test, cyber operations of non-state actors could only be attributable to the state if the relationship is of such complete dependence that it would be right to equate the non-state actors with an organ of the state.[14] Heavy financial subsidies and other support such as the training, arming, equipping and organizing of non-state actors by states are insufficient for attribution or the finding that the state directed or controlled the cyber operation under Article 8 of ARSIWA.[15]

The *Tadic* overall control test provides a lower threshold, in that it is necessary to prove that the state exercised some measure of authority over non-state actors and it issued specific instructions to them concerning the performance of cyber operations, or that it ex post facto publicly endorsed those acts. Given the advantage of plausible deniability, states have no incentive to publicly endorse cyber operations. While it may be possible to attribute non-state conduct to a state under *Tadic*, the International Court of Justice (ICJ) has not accepted the overall control test in interstate disputes.[16] Among the reasons offered by the ICJ are that the test was employed for the purpose of determining whether an armed

[11] International Law Commission (ILC) 'Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries' (2001) 43.
[12] Tim Maurer, *Cyber Mercenaries: The State, Hackers, And Power* (Cambridge University Press 2018) 16-17.
[13] *Prosecutor v Duško Tadic* (Judgment) ICTY-94-1-A (15 July 1999) [120]-[123].
[14] *Nicaragua* (n 8) [109]-[110], see also *Bosnian Genocide* (n 10) ICJ [399]-[400].
[15] ibid, [109]-[110], [115].
[16] *Bosnian Genocide* (n 10) [403].

conflict was international and that the test broadens the scope of state responsibility beyond the fundamental principle of international responsibility, namely that states are responsible only for their own conduct.[17] Moreover, the ILC has noted that the overall control test is "directed to issues of individual criminal responsibility, not State responsibility."[18]

**Problems with classifying cyber operations as breaches of international obligations**

Apart from attribution, cyber operations have to constitute a breach of an international obligation of the state for them to be considered an internationally wrongful act of states. Three internationally wrongful acts are examined. These are prohibited "use of force", as well as violations of the non-intervention and self-determination principles.

*(A.) Cyber operations as prohibited "use of force"*

Article 2(4) of the UN Charter stipulates that member states "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." While cyber operations that cause substantial physical damage may breach the prohibition on the use of force, cyber operations that cause non-physical economic and political disruption do not constitute "use of force".

*(A.1) Plausibility and limits of classifying cyber operations that cause substantial physical damage as "use of force"*

The Tallinn Manual classifies cyber operations as constituting "a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[19] The Manual represents the effects-based interpretation of Article 2(4) of the UN Charter. The physical consequences, not the method of an operation, determine whether cyber operations amount to a "use of force".[20]

[17] ibid [403], [404], [406].
[18] ILC (n 11) 48.
[19] Schmitt (n 1) 330-337.
[20] ibid 328.

Should a particular cyber operation result in substantial physical damage to civilian life and property, the operation would violate the prohibition on the use of force. The effect-based interpretation has validated in the *Legality of the threat of use of Nuclear Weapons* Advisory Opinion, in which the ICJ stated that UN Charter Article 2(4) applies to "any use of force, regardless of the weapons employed" even though it "neither expressly prohibits, nor permits, the use of any specific weapon".[21]

Although there appears to be an emerging academic consensus that cyber operations that result in substantial physical damage can constitute "use of force",[22] there are limits to the interpreting the "use of force" in terms of its physical consequences, as opposed to the use of kinetic weapons that results in physical damage. In other words, the correct albeit stricter interpretation of Article 2(4) would take into account the modality *and* the physical impact of the weapon. This implies that cyber operations, including those that result in physical damage, do not constitute "use of force" as their modality is not kinetic in nature. The effects-based interpretation "represents a hard break from the Charter's instrument-based approach and thereby relies on inherently subjective assessments among states that have divergent strategic capabilities, vulnerabilities, and interests."[23] The UN Charter was drafted at a time when there exists the kinetic nature of a weapon directly corresponded with its physical impact. Cyber operations do not fit into this paradigm. As non-kinetic weapons with the potential to inflict substantial physical damage, cyber operations do not clearly constitute a "use of force" even if they inflict substantial physical damage. For instance, the effects-based interpretation would classify the cyber operation 'Stuxnet', which destroyed Iranian nuclear facilities through the use of malicious computer code, as no different from a missile bombing of the same Iranian facilities. Despite its physical impact, "Stuxnet has not been definitely identified as a use of force by any State and seems unlikely to be."[24]

---

[21] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* [1996] ICJ [39].
[22] Johann-Christoph Woltag, 'Cyber Warfare', *Max Planck Encyclopedia of Public International Law* (2015) Oxford Public International Law 8.
[23] Andrew C. Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate', (2012) 67 Joint Force Quarterly 40.
[24] François Delerue, 'Emerging Voices: Cyber Operations And The Prohibition Of The Threat Of Force' (*Opinio Juris* 2014) <http://opiniojuris.org/2014/07/21/emerging-voices-cyber-operations-prohibition-threat-force/> accessed 14 May 2019.

Notwithstanding the original intent of the UN Charter drafters, the crucial challenge facing the effects-based interpretation is that there is a lack of state practice and *opinio juris* with respect to classifying cyber operations as a "use of force" even if they result in physical damage. The requirement of actual state practice and *opinio juris* is highlighted by the exclusion of economic sanctions from the scope of the use of force even though "from an effects-based perspective, comprehensive and long term economic sanctions can be as severe as the use of force" and "as devastating as the effects of war".[25] If effects were the only yardstick in determining what constitutes "use of force", there is no justification to exclude economic sanctions. Even if one accepts that the modality of weapons is not a necessary criterion of Article 2(4), cyber operations have yet to be accepted as "use of force".

A common argument in favour of the effects-based interpretation is that the deployment of non-explosive weapons such as bacteriological, biological, and chemical devices conceivably amount to the use of force because of its physical impact on life and property.[26] Nevertheless, this argument ignores the widespread state practice and *opinio juris* against the deployment of such devices. In contrast to the cyber operations, multilateral instruments such as the 1972 Biological Weapons Convention and the 1997 Chemical Weapons Convention indicate international agreement on the prohibition of using such weapons even for war purposes. Multilateral conventions may play an important role in "recording and defining rules deriving from custom".[27] In contrast, there is no internationally agreed upon definition of what cyber operations constitute "cyber attacks". Even theoretical attempts to prove that cyber warfare should qualify as armed conflict within the context of the use of force under Article 2(4) "have not so far been accepted generally."[28] Due to the lack of any state consensus on definitions and the threshold of physical impact that would qualify a cyber operation as a use of force, whether a cyber operation would constitute a use of force would vary from state to state and their particular strategic interests.

---

[25] Cassandra LaRae-Perez, 'Economic Sanctions as a Use of Force: Re-evaluating the Legality of Sanctions from an Effects-Based Perspective' (2002) 20 Boston University International Law Journal 163, 180.
[26] Ian Brownlie, *International Law And The Use Of Force By States* (8th edn, Oxford University Press 2012) 362.
[27] *Continental Shelf (Libyan Arab Jamahiriya/Malta)* (Judgment) [1985] ICJ Rep 13 [2].
[28] Jozef Valuch, Tomáš Gábriš and Ondrej Hamuľák, 'Cyber Attacks, Information Attacks, And Postmodern Warfare' (2017) 10 Baltic Journal of Law & Politics 67.

*(A.2) Cyber operations that cause non-physical damage do not constitute "use of force"*

The prevailing focus on cyber operations inflicting substantial physical damage may be misplaced. The focus should instead be on cyber operations that cause political and economic disruption. As cyber operations are auxiliary tools that supplement traditional conventional weapons, it is unlikely that a standalone 'cyber war' will happen and situations where cyber operations are deployed to inflict physical damage are likely to be those involving conventional warfare.[29] Moreover, the advantage of cyber operations precisely lies in their capacity to inflict costs short of the widespread civilian damage arising from conventional warfare, which has become politically and militarily risky in a geopolitical environment stabilized by nuclear weapons. Akin to sub-conventional warfare tactics such as terrorism, cyber operations allow states to gain strategic advantages without risking full-blown conventional war. Cyber operations inflicting economic and political disruption, rather than substantial civilian damage, are a likelier threat to international peace and stability.

Economically, cyber operations can destabilize the economic system of states by disrupting financial institutions such as banks and businesses. Cyber operations can obstruct economic activity and undermine economic confidence through cyber attacks on payment systems, manipulating, altering and corrupting financial data, as well as impairing the wide infrastructure, such as telecommunications, that the financial system depends upon.[30] For instance, the North Korean Lazarus Group "routinely looks for ways to compromise banks and exploit crypto currencies".[31] In 2007, Russian-distributed denial of service (DDoS) cyber attacks on Estonia not only shut down the websites of its government ministries, banks, and political parties, but also disabled its

[29] Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35 Journal of Strategic Studies 29. See also Erik Gartzke, 'The Myth Of Cyberwar: Bringing War In Cyberspace Back Down To Earth' (2013) 38 International Security 66.
[30] Martin Boer and Jaime Vazquez, 'Cyber Security & Financial Stability: How Cyber-Attacks Could Materially Impact The Global Financial System' (2017) The Institute of International Finance 4-7.
[31] Paul Mee and Til Schuermann, 'How A Cyber Attack Could Cause The Next Financial Crisis' (2019) Harvard Business Review.

parliamentary email server, the IT capabilities of its ministries, and even prevented credit card transactions for several days.[32]

On the other hand, cyber operations can disrupt the internal political affairs of a state by undermining public trust in state institutions, aggravate social discord and spur separatist or anti-establishment movements through information technology. Methods used by cyber operations include using fake social media account 'trolls' and automated account 'bots' to spread 'fake news' or divisive content as well as the leaking of politically damaging information acquired through hacking and spear phishing.[33] Furthermore, political disruption has military implications. As observed in the 2014 Russian-Ukrainian conflict, the political disruption caused by such cyber operations can also weaken military capabilities of a state by undermining public support for military actions through the online spreading of disinformation to discredit governmental actors and aggravate civil distrust.[34] Such impacts are psychological in nature; they do not involve direct and violent physical damage. More severe interference can encompass cyber hacking of electoral systems and databases, compromising the integrity of political processes of states.

Such cyber operations, however, do not fall within the scope of the "use of force" under Article 2(4) of the UN Charter even if the effects-based interpretation of "use of force" were accepted. Cyber operations that cause non-physical damage, especially economic and political disruption, would not constitute an illegal "use of force". This is because "force" in Article 2(4) does not include economic and political disruption.

According to Article 31(1) of the Vienna Convention on the law of treaties (VCLT), the meaning of "force" in Article 2(4) has to be interpreted within the "context and in light of [the UN Charter's] object and purpose." In interpreting the context of the treaty's purpose, reference is made to the treaty's preamble.[35]

---

[32] Stephen Herzog, 'Revisiting The Estonian Cyber Attacks: Digital Threats And Multinational Responses' (2011) 4 Journal of Strategic Security 51, 52.
[33] Alina Polyakova and Spencer Boyer, 'The Future Of Political Warfare: Russia, The West, And The Coming Age Of Global Digital Competition Report' (The Brookings Institution 2018) 4, 9.
[34] Yuriy Danyk, Tamara Maliarchuk and Chad Briggs, 'Hybrid War: High-Tech, Information And Cyber Conflicts' (2017) 16 Connections: The Quarterly Journal 14
[35] Vienna Convention on the law of treaties 1969, art 31(2).

The preamble of the UN Charter calls on states to ensure that "armed force shall not be used". The term "force" is referenced in Articles 41, 44 and 46, which all contextualize "force" in terms of *armed* force. The ICJ in *Nicaragua* ruled that the "prohibition of the use of force is to be considered in the light of other relevant provisions of the Charter."[36] In addition, the *travaux preparatoires* of the UN Charter show that the proposal to expand the ambit of Article 2(4) to include economic and political coercion was "decisively defeated".[37] During the 1945 San Francisco Conference, the majority of states rejected the 1945 Brazilian, Ecuadorian and Iranian proposals to expand the meaning of "force" to encompass economic and political coercion.[38]

This restrictive interpretation of "force" as armed force is further affirmed by later UN resolutions such as the 1970 Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations,[39] 1974 Declaration on the Definition of Aggression,[40] and the 1987 Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations.[41] In fact, when deciding a draft paralleling UN Charter Article 2(4), the UN Commission on Friendly Relations rejected arguments that "force" encompassed all forms of political and economic pressure.[42]

Although such cyber operations are not prohibited "use of force", they may conceivably violate international legal principles of non-intervention and self-determination. This paper will now analyze the possibility and the limits of relying on these two principles in regulating cyber operations that cause economic and political disruption. The next two sections will solely focus on cyber operations that disrupt the economic and political systems of states.

---

[36] *Nuclear Weapons* (n 21) [38].
[37] Michael Schmitt, *Proceedings Of A Workshop On Deterring Cyberattacks* (National Academies Press 2010) [154]-[155].
[38] James Green, 'The Regulation Of Cyber Warfare Under The Jus Ad Bellum', *Cyber Warfare: A multidisciplinary analysis* (Routledge Studies in Conflict, Security and Technology 2015) 101.
[39] United Nations General Assembly, 26/25 (XXV), 24 October 1970.
[40] United Nations General Assembly, 3314 (XXIX), 14 December 1974.
[41] United Nations General Assembly, A/RES/42/22, 18 November 1987.
[42] Christopher Yoo, 'Cyber Espionage Or Cyberwar?: International Law, Domestic Law, And Self-Protective Measures', *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 178.

*(B) Cyber operations as a violation of the principle of non-intervention*

The principle of non-intervention entails "the right of every sovereign State to conduct its affairs without outside interference".[43] As an expression of sovereign equality of states and an embodiment of respect for territorial sovereignty,[44] the principle of non-intervention is part of customary international law.[45] The non-intervention principle forbids states to "intervene directly or indirectly in internal or external affairs of other States".[46] Political and economic disruption arguably violate the non-intervention principle because a prohibited intervention is one that uses coercion to interfere in matters in which a state has sovereignty to decide freely, of which includes "the choice of a political, economic, social and cultural system."[47]

Various United Nations General Assembly (UNGA) Resolutions indicate that the principle of non-intervention is applicable to cyber operations that interfere in the internal political and economic affairs of states. Although non-binding, UNGA Resolutions are "not wholly without normative force" because they "form part of the broader normative context within which expectations of what is reasonable or proper State behavior are formed."[48] The 1965 Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty stipulates that "no State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any State."[49] The Declaration also declared that no states might "use or encourage economic, political or *any other type* of measures to coerce another State" to secure *any kind* of advantages from it.

Similarly, the 1970 Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States affirms that the duty of non-intervention requires states to refrain from "*all other forms* of interference" against the "political, economic and cultural elements" of a state

[43] *Nicaragua* (n 8) [202].
[44] Malcolm N Shaw, *International Law* (6th edn, Cambridge University Press 2008) 1148.
[45] *Nicaragua* (n 8) [202]. See also *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ [164].
[46] *Nicaragua* (n 8) [205].
[47] ibid [205].
[48] Vaughan Lowe, *International Law* (Oxford University Press 2007) 95, 96.
[49] United Nations General Assembly, 2131 (XX), 21 December 1965.

because such interference violates a state's "inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State".[50] In fact, the 1970 Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States represents "a consensus" on "the fundamental principles upon which the international legal order is based", of which the non-intervention principle is one of the seven "irreducible core of principles".[51] The 1976 Declaration on Non-interference in the Internal Affairs of States similarly condemns the "all forms of overt, subtle and highly sophisticated techniques of coercion, subversion and defamation aimed at disrupting the political, social or economic order of other states."[52] These instruments suggest that there is no restriction as to the form of interference and the impacts of interference encompass more than direct military force. Therefore, cyber operations that disrupt the economic and political systems of states arguably violate the non-intervention principle. There are, however, two limits to using the non-intervention principle.

First, the non-intervention principle and international law are ill equipped to take into account the kinds of coercion present in politically disruptive cyber operations. The element of coercion "defines, and indeed forms the very essence of, prohibited intervention" and uses force.[53] Cyber operations that seek to alter preferences of an electoral or undermine domestic confidence in a government do not involve compulsion of a state to act or choose in one way or another. Internationally recognized forms of coercion, such as retorsion, reprisals, economic sanctions, and the direct or indirect use of armed force,[54] entail observable and tangible measures that influence a state's actions overtly. Politically disruptive cyber operations are, however, harder to prove and quantify. Such operations may not even involve observable conflicts of compulsion because they insidiously alter a people's political preferences by shaping their perceptions, beliefs and cognitions online in such a way that they unconsciously accept certain orders of things.[55] For instance, foreign cyber operations have shaped public opinion and undermined democratic processes during the Brexit

[50] United Nations General Assembly, 2625 (XXV), 24 October 1970, Principle 3.
[51] Lowe (n 48) 100.
[52] United Nations General Assembly, 31/91, 14 December 1976.
[53] *Nicaragua* (n 8) [205].
[54] Christopher Joyner, 'Coercion', *Oxford Public International Law* (Max Planck Encyclopedia of Public International Law 2006) [1]-[15].
[55] Steven Lukes, *Power* (Palgrave Macmillan 2006) 28.

referendum and the 2016 presidential elections. These operations manipulated social media algorithms by utilizing bots to feign the popularity of particular politicians and political views through increased followers and 'likes', drowning out political hash tags, and online smear campaigns.[56] Therefore, online electioneering aimed at influencing and altering an electorate of another state does not meet the high threshold of coercion and does not violate the non-intervention principle.

Second, classifying cyber operations as violations of the non-intervention principle rather than "use of force" limits the effectiveness of international law in regulating and deterring cyber operations. Moreover, there are different legal implications of classifying cyber operations as violations of non-intervention instead of Article 2(4). While non-intervention is characterized as customary international law, the prohibition on the use of force under Article 2(4) is *jus cogens*,[57] ranking higher than treaty law and customary international law in the international hierarchy of norms.[58] *Jus cogens* norms are non-derogable[59] and bind states regardless of consent and state practice.[60] The ICJ in *Nicaragua* stressed the necessity of distinguishing between armed attacks, which are "the most grave forms of the use of force" from "other less grave forms".[61] This difference in gravity arguably accounts for the varying legal consequences between breaching the non-intervention principle and the prohibition on the use of force. In situations involving breaches of the non-intervention principle, victim states are

---

56 Philip N. Howard, Samuel Woolley and Ryan Calo, 'Algorithms, Bots, And Political Communication In The US 2016 Election: The Challenge Of Automated Political Communication For Election Law And Administration' (2018) 15 Journal of Information Technology & Politics 82, 83, 86.

57 International Law Commission, 'Draft articles on the law of treaties with commentaries', *Yearbook of the International Law Commission Volume II* (1966) 247. See also *Nicaragua* (n 8) [190], [202].

58 *Prosecutor v Anto Furundžija* (Trial Chamber Judgment) ICTY IT-95-17/1-T (10 December 1998) [153]. See also Dire Tladi, 'Third Report On Peremptory Norms Of General International Law (Jus Cogens)' (International Law Commission 2018) [140].

59 Vienna Convention on the law of treaties 1969, art 53. See also Dinah Shelton, 'Normative Hierarchy In International Law' (2006) 100 American Journal of International Law 297.

60 Asif Hameed, 'Unravelling The Mystery Of Jus Cogens In International Law' (2014) 84 British Yearbook of International Law 64-68, 98. See also Thomas Kleinlein, 'Jus Cogens as the 'Highest Law'? Peremptory Norms and Legal Hierarchies' (2015) 46 Netherlands Yearbook of International Law 197.

61 *Nicaragua* (n 8) [191].

generally restricted to non-forcible countermeasures whereas states can respond forcibly with graver countermeasures in cases involving the use of force.[62] Self-defence under Article 51 of the UN Charter necessarily requires 'armed attack'; violation of non-intervention principles through economically or politically disruptive cyber operations does not suffice. The necessity of 'armed attack' hence "constitutes an integral part of Article 51; no self-defence can be exercised if no armed attack occurs."[63] In the *Wall* Advisory Opinion, the ICJ affirmed that the right of self-defence only exists in the case of an armed attack by one state against another.[64] The fact that cyber operations do not meet the threshold of 'armed attack' under Article 51 due to a lack of physical damage undermines the deterrence capacity of the non-interference principle. Unlike the prohibition on the use of force, which can trigger the right to individual or collective self-defence against cyber operations that inflict substantial physical damage, violations of non-interference can best allow non-forcible countermeasures.

Such threats fail to deter states from interfering in the political and economic systems through indirect, non-military means. This is evident from how the non-intervention principle is "has long been regularly breached by states – at least in relation to the 'non-forcible' actions that it covers – without much in the way of legal, or even political, consequence" and still "struggles to restrain state behaviour".[65] As *jus cogens*, the use of force is particularly perceived negatively, especially in light of its direct destructive physical impacts on life and property.[66] In contrast, while economic or political consequences can be disruptive or destabilizing, they "emerge much more slowly, and thereby allow opportunity for reflection and resolution, compounds the danger of escalation."[67] Therefore, while cyber operations can breach the non-intervention principle, the varying legal

[62] Christian Henderson, 'The Provision of Arms and Non-Lethal Assistance to Governmental and Opposition Forces' (2013) 36 University of New South Wales Law Journal 651.
[63] Tom Ruys, *'Armed Attack' And Article 51 Of The UN Charter* (Cambridge University Press 2013) 67.
[64] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ [139].
[65] Green (n 38) 109-110.
[66] Henderson (n 62) 652.
[67] Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law 911-912.

status and its concomitant legal consequences mean that impunity is likely to persist.

*(C) Cyber operations as violations of the principle of self-determination*

Self-determination is another principle that may be used to regulate economically and politically disruptive cyber operations. Enshrined in Article 1(2) of the UN Charter, the right to self-determination is a customary norm.[68] Principle 5 of the Declaration on the Principles of International Law concerning Friendly Relations and Co-operation among States stipulates, "all peoples have the right freely to determine, without external interference, their political status and to pursue their economic, social, and cultural development".[69] Cyber election meddling is violates the right to of self-determination because its application "requires a free and genuine expression of the will of the peoples concerned."[70] After all, self-determination is "a legal concept that captures the right of a people to decide, for themselves, both their political arrangements (at a systematic level) and their future destiny (at a more granular level of policy)."[71]

A limiting factor is that this principle has largely been situated in the context of decolonization and the right of "non-self-governing territories" to emerge as sovereign, independent states.[72] Specifically, the customary status of self-determination is confined to "the right to territorial integrity of a non-self-governing territory as a corollary of the right to self-determination."[73]Although the ICJ has seemingly applied self-determination principles beyond decolonization situations to include the right of the Palestinian people to self-determination,[74] it is still applied in terms of *territorial statehood*, not psychological manipulation or election meddling.

---

[68] *Legal Consequences of the Separation of the Chagos Archipelago from Mauritius in 1965 (Advisory Opinion)* [2019] ICJ [152].
[69] United Nations General Assembly, 2625 (XXV), 24 October 1970.
[70] *Western Sahara (Advisory Opinion)* [1975] ICJ [55].
[71] Jens David Ohlin 'Did Russian Cyber Interference in the 2016 Election Violate International Law' (2017) 95 Texas Law Review 1580.
[72] *Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970) (Advisory Opinion)* [1971] ICJ [52]. See also *Western Sahara* (n 70) [54] and *Chagos* (n 68) [160].
[73] *Chagos* (n 68) [160].
[74] *Wall* (n 64) [115], [118].

Even if the applicability of self-determination is expanded to situations beyond the decolonization context, reliance on self-determination as a regulatory principle faces the same limits as non-intervention, particularly with respect to self-defence under Article 51. This is because in cases where self-determination is applied to existing states, the "principle of self-determination normally takes the well-known form of the rule preventing intervention in the internal affairs of a State, a central element of which is the right of the people of the State to choose for themselves their own form of government."[75] This specific application of self-determination, however, faces the same aforementioned limits as non-intervention.

## II. INTERNATIONAL HUMANITARIAN LAW AND CHALLENGES POSED BY CYBER OPERATIONS

The use of cyber operations in situations of armed conflicts ("cyber warfare") also presents new challenges to IHL. Cyber warfare refers to the "means and methods of warfare that consist of cyber operations amounting to, or conducted in the context of, an armed conflict, within the meaning of IHL."[76] Cyber operations can be used as a standalone tool of armed conflict, or to complement conventional warfare. In both circumstances, cyber operations pose unique challenges to the application and effectiveness of IHL. Despite the customary legal status of the Martens clause, which stipulates that IHL also applies to new technologies,[77] the *character* of cyber warfare and the *nature* of societies in which cyber warfare is conducted pose unique challenges to the effectiveness of IHL in achieving its purpose of limiting the destructive effects of armed conflict.

[75] James Crawford, *The Creation of States in International Law* (Oxford University Press, 2007) 126.

[76] Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 International Review of the Red Cross 538. See also International Committee of the Red Cross, 'Cyber warfare and international humanitarian law: The ICRC's position' (2013) 1.

[77] International Committee of the Red Cross, 'Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949' (1987) 39.

**How the character of cyber warfare challenges the applicability of IHL**

The involvement of non-state actors and the loose and clandestine relationships between the state and non-state actors in cyber warfare inhibits the legal capacity of the IHL to constrain the effects of armed conflicts. Similarly, the use of non-state actors poses the serious challenge of legal attribution.

IHL applies to two types of armed conflicts, namely International Armed Conflicts (IAC) and Non-International Armed Conflicts (NIAC). As IAC only applies to armed conflicts between states, for IHL to *even apply* in cyber warfare involving non-state actors, the cyber conduct of non-state actors has to be attributable to the state. Legal attribution enables the conflict to be classified as an IAC, which then triggers the applicability of IHL. As previously argued, legal attribution is a challenge. In an IAC where states tacitly support non-state actors, the legal difficulty of attribution would imply that IHL is inapplicable to conduct by non-state actors.

An even more challenging IAC situation would be voluntary civilian participation in hostilities *without any* state support. This is a likely situation because compared to conventional weaponry, there are lower financial barriers to conducting cyber warfare and cyber methods are more accessible online. Such low barriers to entry into cyberspace mean that civilians can easily conduct hostile cyber operations against the hostile state. Direct civilian participation in hostilities could increase civilian causalities by justifying retaliatory cyber operations. This is because direct civilian participation removes their protection from attacks.[78] Direct civilian participation in cyber warfare also challenges the direct applicability of IHL because such attacks by civilians are not attributable to the state. Apart from challenging the relevancy of IHL's conceptualization of armed conflicts as either IAC or NIAC, the difficulty of attribution problematizes the application of the IHL in cyber warfare. Even if cyber operations by non-state actors inflict significant damage to civilian objects, legal attribution problems challenge the applicability and relevancy of IHL in limiting humanitarian costs.

As only armed conflicts between a state and an *organized* armed group qualify as NIACs, for IHL to *even apply* in such a cyber warfare scenario, the non-state

[78] Additional Protocol 1 (AP 1) art 51(3).

actors must have some form of organization.[79] A minimum level of organization would exist if the group had a hierarchical command structure, disciplinary rules, and the ability to determine a unified military strategy.[80] These actors, however, are unlikely to be organized as virtual groups; they are linked only by online communication and group members may not know each other.[81] This implies that the non-state actors involved in civil conflicts would not be held liable under IHL even if they were to cause widespread civilian causalities by damaging nuclear power plants, dams, air traffic control systems, transportation, and satellites through disruptive cyber operations.

Furthermore, the convergence between artificial intelligence (AI) and cyber warfare would create serious legal attribution and responsibility issues under IHL. Cyber warfare conducted by AI-driven machine learning computers and malicious malware can autonomously identify and exploit system vulnerabilities, thereby possessing sophisticated capacity to inflict greater civilian casualties. Additionally, autonomous robots, rather than human soldiers, may increasingly be the actors conducting cyber warfare.[82]

Apart from the challenge of determining which actor should be legally responsible for IHL violations caused by autonomous cyber warfare weapons, another challenge is the difficulty of determining the legality of new methods of warfare under Article 36 of Additional Protocol 1 (AP1), especially where AI cyber weapons continuously learn, adapt and evolve as they interact with their environment.[83] In other words, as AI cyber weapons constantly undergo transformation in their lethal capabilities in reaction to changing military situations, it is challenging, if not impossible, to pin down or review the exact lethal capability of the weapon at any point in time. As these malicious cyber bugs and codes operate autonomously, they may lead to indiscriminate civilian impacts in both the targeted state and third-party states that are uninvolved in the conflict.

---

[79] Additional Protocol 2 (AP 2) art 1.
[80] *Prosecutor v. Ljube Boskoski Johan Tarculovski (Trial Chamber Judgment)* ICTY IT-04-82-T (2008) [194]-[203].
[81] Eitan Diamond, 'Applying International Humanitarian Law to Cyber Warfare' (2014) 67 Law and National Security: Selected Issues 74.
[82] Kriangsak Kittichaisaree, *Public International Law Of Cyberspace* (Springer 2019) 231.
[83] 'The Weaponization Of Increasingly Autonomous Technologies: Autonomous Weapon Systems And Cyber Operations' (The United Nations Institute for Disarmament Research 2017) 7.

Automated retaliatory "hacking back"[84] cyber attacks that inflict severe civilian causalities also complicate legal attribution and responsibility.

## How cyber warfare in technologically advanced societies challenges IHL principles

### *Distinction*

The changing nature of society due to technological advancements problematizes the application of IHL in cyber warfare. In the Internet of Things (IOT) society, dual use infrastructure and the interconnectivity between critical civilian infrastructure and cyber Internet systems challenge the application of the IHL rules of distinction and discriminate attacks. By blurring the line between military and civilian targets, dual use objects and IOT facilities complicate efforts to determine if a cyber operation constitutes a violation of IHL. Since such blurring is very much a consequence of technological progress, establishing that a state intentionally integrated its civilian and military facilities so as to deter and shield its military objectives from attacks is difficult, if not impossible. This problematizes the application of IHL rules, namely precaution against locating military objectives within densely populated civilian areas[85] and attacks on civilian objects.[86] As dual use infrastructure can simultaneously possess civilian and military functions, this also poses challenges to the determination of when a civilian object loses its "civilian character and qualifies as a military objective" that is liable to attack.[87] This is especially so when facilities that are originally designed for civilian uses have military roles, and vice versa.

### *Discriminate attacks*

Given that the "definition of indiscriminate attacks is an implementation of the principle of distinction",[88] the challenges facing the IHL distinction also problematize the prohibition against indiscriminate attacks, which are attacks not

[84] Paul Scharre, *Army Of None* (W W Norton & Company 2018) ch 14.
[85] AP 1. Art 58.
[86] AP 1. Art 52.
[87] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law: Volume 1* (Cambridge University Press 2005) 34 (Rule 10).
[88] ibid 43 (Rule 13).

directed at a specific military objective.[89] The difficulty in conducting warfare at specific military objects is due to the phenomenon of 'civilian creep', where accelerated permeation of advanced technologies into every civilian aspect of society obstructs accurate targeting.[90] Given the interconnectivity between cyber and civilian infrastructure, even when cyber operations are precisely targeted at specific military objects that "by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage",[91] they could trigger severe collateral impacts on civilian lives and objects.

Additionally, cyber warfare in an IOT society also introduces new objects vulnerable to armed attack. During cyber warfare, cyber operations can alter, manipulate or even destroy civilian data, including electoral votes, health records, and banking account information. Although destroying or altering data may not lead to direct physical harms, such cyber operations during warfare do not only impede or disrupt governmental functions, but are also contrary to military necessity[92] and general protection of civilian objects.[93] In a cyber-dependent IOT society, an acute challenge would be to reconsider and debate the interpretation of "civilian objects" in the context of the object and purpose of IHL in protecting civilians from the scourge of warfare.[94] Moreover, under IHL, the damage to civilian objects arguably does not necessarily need to entail a violent physical impact on civilian lives. As evident from article 53 of AP1, which prohibits "any acts of hostility directed against the historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples", the focus of IHL is on limiting the collateral effects of warfare on the civilian population. The challenge of re-examining what kinds of civilian objects in IOT society

[89] AP 1. Art 51(4)(a).
[90] Robert McLaughlin and Hitoshi Nasu, 'Introduction: Conundrum Of New Technologies In The Law Of Armed Conflict', *New Technologies and the Law of Armed Conflict* (Springer 2014) 9.
[91] AP 1. Art 52(2).
[92] Michael N Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' (2014) 25 Stanford Law and Policy Review 295.
[93] AP 1. Art 52(1) and 52(3).
[94] 'The Conduct Of Hostilities And International Humanitarian Law: Challenges Of 21St Century Warfare' (Stockton Center for the Study of International Law 2017) 339.

require protection from cyber operations is pertinent if IHL were to fulfil its important purpose of "the safeguarding of the lives *and dignity* of human beings".[95]

*Proportionality*

'Civilian creep' also poses challenges to the IHL rule of proportionality, which prohibits excessive civilian costs in relation to concrete and direct military advantage.[96] Cyber operations' direct impacts may be nonlethal or temporary, but they may indirectly result in severe civilian harms.[97] For example, while cyber operations may inconvenience the civilian population by temporarily disabling Internet information transmission, such operations may cause the loss of lives because hospitals are unable to communicate vital information.[98] As such, the direct impacts of cyber operations may be proportionate to the military advantage gained, but the indirect impacts may be *unexpectedly* disproportionate even when feasible precautions[99] are taken. Proportionality is "couched in the language of expectation and anticipation" or "what is reasonably foreseen in advance of an attack"; therefore "what is 'excessive' collateral damage to civilians/civilian objects is determined on the basis of the original expectation (of the collateral damage) and anticipation (of the military advantage) as formed before, not after, the damage".[100] The interconnectedness between cyber and civilian infrastructure problematizes the task of determining whether a cyber operation is proportionate. It also poses the challenge that cyber operations may still result in disproportionate civilian costs even if there is adherence to IHL proportionality standards. Therefore, IHL rules may not be sufficient in limiting excessive civilian costs arising from cyber warfare.

---

[95] Jean S Pictet, *Commentary I on the Geneva Convention* (International Committee of the Red Cross 1952) 12.
[96] AP 1. Art 51(5)(b) and 57(2)(iii). See also Michael N Schmitt, *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations* (Cambridge University Press 2017) 470-475.
[97] Oona A Hathaway, Rebecca Crootof, William Perdue, and Philip Levitz, 'The Law of Cyber-Attack' (2012) 100 California Law Review 851.
[98] ibid 851.
[99] AP 1. Art 57(2).
[100] Yoram Dinstein, 'The Principle Of Distinction And Cyber War In International Armed Conflicts' (2012) 17 Journal of Conflict and Security Law 270.

**Proposal: International independent fact-finding body**

This essay proposes that an international independent fact-finding body be established to address the limitations faced by international law in regulating the use and conduct of cyber operations. This body's primary purpose is to investigate and identify the actors responsible for cyber operations. It would also identify the economic and political impacts and the specific IHL violations arising from these particular operations. After independent investigations, the body will publish its findings. This proposed body would focus on fact-finding and will not have prosecutorial or enforcement capabilities akin to the International Criminal Court. Upon the publication of the investigation report, the victim state, not the body, will decide whether to respond and if it chooses to do so, it will decide on the kind of legal remedies and punitive measures, including individual or collective sanctions, arbitration, or litigation.

Granting the body jurisdictional capabilities over international law violations arising from cyber operations would face significant difficulties in acquiring state consent. Furthermore, even if the body had prosecutorial powers, it could not compel states to surrender individuals responsible for particular cyber operations. By providing information and removing anonymity, fact-finding plays an indispensable role in crystalizing international legal *norms* and creating *taboos* surrounding the use and conduct of cyber operations in the long term. This challenges the notion that prosecutorial or enforcement capabilities are necessary to constrain state behaviour.

Regarding the conduct of cyber operations, this fact-finding body can reduce the legal ambiguity surrounding the application of IHL in contexts of cyber warfare. With respect to the conduct of cyber operations in warfare situations, the detailing of the humanitarian impacts of cyber operations is required to categorize specific types of cyber warfare as violations of IHL. Although this body does not have prosecutorial or enforcement powers, it can still contribute to greater clarity and consistency in how IHL applies to cyber warfare, thereby minimizing legal ambiguity. Greater clarity arising from the body's investigative reports can constrain and structure the conduct of cyber warfare in accordance with IHL rules. Even though the body's reports are non-binding, they can set soft law standards for states to reorient and adjust their cyber warfare conduct. This is possible because "much norm advocacy involves pointing to discrepancies

between words and actions and holding actors personally responsible for adverse consequences of their actions", in other words, the body functions by providing "the information and publicity that provoke cognitive dissonance among norm violators."[101] Examples of such bodies, which offer non-enforceable yet norm-contributory reports, include the complaint mechanisms of the United Nations Special Rapporteurs, Working Groups, and Human Rights treaties. In the long run, the normalization of IHL rules in cyber warfare contexts may facilitate the creation of multilateral treaties, which restrict or prohibit the use of certain cyber warfare operations and particular cyber warfare targets.

With respect to the use of cyber operations, this fact-finding body can potentially constrain states from even using cyber operations. As previously argued, given the difficulties of classifying cyber operations as internationally wrongful acts of a state under international law, it is currently practically and theoretically difficult to rely on international law, namely the prohibition on the use of force, non-intervention, and self-determination, to outlaw or prohibit cyber operations as internationally wrongful acts. If so, *jus ad bellum* arguably does not offer a fruitful approach in protecting international peace and security from cyber operations. Rather than attempting to theoretically fit cyber operations into the legal frameworks of "use of force" or drafting a new treaty stipulating the conditions under which the use of cyber operations is legally permissible, a more effective approach would be to capitalise on incipient international *norms* of sovereignty and non-intervention to 'name and shame' economically and politically disruptive cyber operations. To utilize such stigmatizing effects of international legal norms, the identification of culpable actors is necessary. This is because "norms cannot get much purchase in a world without serious attribution" as "anonymity is a norm destroyer."[102] Through fact-finding investigations and monitoring, this body removes anonymity.

The importance of the body's monitoring function can also be elucidated with reference to how international monitoring entities are most needed in international issues that have diffused and indirect costs, such as cyber operations that inflict political and economic disruption. In accounting for the kind of

[101] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics And Political Change' (1998) 52 International Organization 904.
[102] Jack Goldsmith, 'How Cyber Changes The Laws Of War' (2013) 24 European Journal of International Law 136.

monitoring arrangements in different international issues, professor Xinyuan Dai offers a framework to do so (Figure 1).[103] The framework first comprises of 'Interest Alignment between Noncompliance Victims and Their State', which refers to states' interests in protecting potential victims of legal non-compliance and this would in turn affect their interests in monitoring instances of non-compliance.[104] Secondly, the 'Availability of Noncompliance Victims as Low-Cost Monitors', which is determined by whether noncompliance imposes direct and easily detectable impacts on victims.[105] As indicated by the top left quadrant in Figure 1, the presence of alignment *and* availability of victims would mean that states and victims would monitor non-compliance. Cyber operations that cause substantial physical damage would fall within this quadrant. This is because not only do states and victims both share an interest in ensuring such operations are unlawful uses of force, the effects are easily and directly felt and seen by the victim population, which would then increase political pressure on states to retaliate or monitor future uses of such operations. In such scenarios where there exists interest alignment between states and cyber victims as well as the easily detectable victim impacts, both states and victims would be incentivized to conduct monitoring and fact-finding. In any case, as previously argued, such cyber operations are likely to be used as complements in conventional warfare and are improbably used as standalone tools.

What then is of interest would be a cyber operation that inflicts non-physical effects. In contrast, while there exists interest alignment, the availability of non-compliance victims is low as the effects of political and economic disruption tend to be diffused, indirect, and covert. If so, monitoring by treaty organizations such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) is necessary. Monitoring by a treaty organization is necessary because it removes states' ability to hide behind masks of anonymity and uncertainty by 'naming and shaming' responsible states. Although this paper's proposed body is *not* a treaty body akin to the NPT, the justification is similar, in that a monitoring body is required in cases where cyber operations inflict non-physical effects.

[103] Xinyuan Dai, 'Information Systems In Treaty Regimes' (2002) 54 World Politics 412.
[104] ibid 408.
[105] ibid 414.

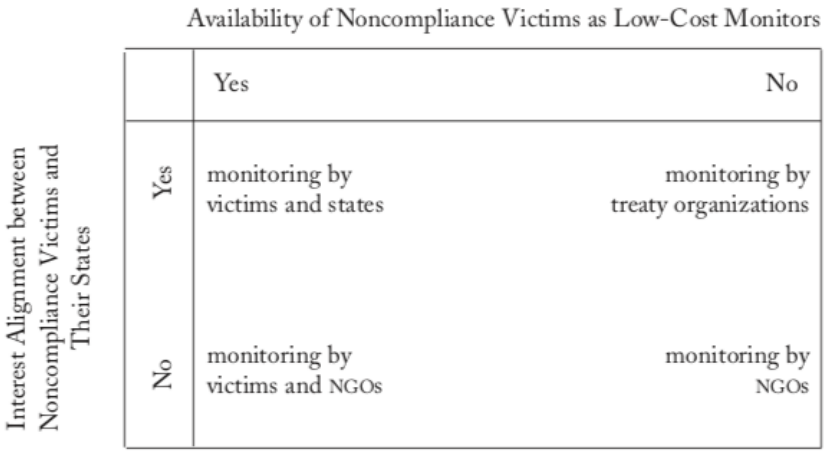


FIGURE 1
ORGANIZATIONAL FORMS OF INFORMATION SYSTEMS

This 'naming and shaming' works because it builds on the incipient international norms of sovereignty and non-intervention. Regardless of the legal consequences, there exists international stigma associated with such actions. This is evident from how the 'nuclear taboo', which refers to the norm prescribing against the use of nuclear weapons, has delegitimized nuclear weapons as weapons of war to such an extent that nuclear weapons remained unused even in cases where the self-interest borne out of mutually assured destruction does not exist; nuclear states such as the United States would rather lose a war than resort to nuclear weapons against non-nuclear states such as Vietnam.[106] By finding attribution through fact-checking, the body crystallizes and capitalizes on the stigma associated with violations of the existing norms of sovereignty and non-intervention to bear upon politically and economically disruptive cyber operations.

Therefore, the theoretical difficulties of applying international law principles in the cyber domain does not preclude the geopolitical reality that the norms associated with such principles influence the normative expectations of interstate relations. For instance, although the international law principle of non-intervention faces theoretical limits in prohibiting cyber election interference,

[106] Nina Tannenwald, *The Nuclear Taboo* (Cambridge University Press 2008) 3, 5, 10, 27.

non-intervention principle still provides a normative framework regulating interstate relations. Actions that violate such a norm are stigmatized regardless of whether they theoretically fit into the non-intervention framework. Such stigma against the use of cyber operations operates through 'outcasting', which is a non-violent way of enforcing international law and norms by denying those who violate international rules and norms the benefits available to the rest of the international community.[107]

Additionally, by investigating and identifying the territorial and political origins of cyber operations, the body can simultaneously contribute to the consolidation of due diligence norms in the cyber domain. Due diligence comprises of the obligation not to allow territory or cyber infrastructure under its governmental control to be used for cyber operations that adversely affect other states.[108] This involves extending the duty to prevent transboundary harm in international environmental law to the domain of cyber warfare. The due diligence obligation to prevent transboundary harm refers to "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[109] This obligation is recognized as "part of the corpus of international law".[110] Such obligations are procedural and require states from which the harm originates to take all possible and appropriate measures to prevent and minimize such harm from causing damage to areas beyond national jurisdiction.[111] Extension of such a principle to cyber warfare would mean that states are expected to be responsible for cyber operations that emanate from their territory even if legal attribution cannot be made out. Such an extension represents a shift from the traditional requirement of attribution for the assignment of state responsibility for internationally wrongful acts under Article 2 of ARSIWA. This lowering of the threshold for assignment of state responsibility is especially pertinent in the cyber domain, where the nature of cyber activity and the relationships between actors involved in cyber operations render technological and legal attribution difficult. Applying this duty would prevent states from

[107] Oona Anne Hathaway and Scott Shapiro, *The Internationalists: How A Radical Plan To Outlaw War Remade The World* (Simon & Schuster) 375.
[108] Schmitt (n 1) 30-42.
[109] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) (Judgment)* [1949] ICJ [22].
[110] *Nuclear Weapons* (21) [29].
[111] International Law Commission, 'Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries' (2001) 148, 153, 154.

masking their cyber warfare operations behind clandestine relationships with non-state actors. Additionally, due diligence addresses situations where states outsource cyber operations to another state or to non-state actors located in another state. Due diligence not only deters states from conducting cyber operations on behalf of other states, but also incentivizes states to ensure that their territory is not used to conduct cyber operations. Moreover, this norm bypasses a crucial challenge posed by cyber operations, namely identification of the location where the operation originated does not offer knowledge of the actors responsible.

The maintenance of international peace and security is a perennial and quintessential challenge facing international law. The indeterminacy of theoretically extending international law to encompass new issues and developments, such as cyber operations, need not require drafting a new international cyber treaty. In any case, a new cyber treaty is politically infeasible. There have been calls for an International Cyber Convention on cyber attacks[112] and a 'Digital Geneva Convention' on the conduct of cyber operations.[113] The geopolitical realities of cyber operations as military strategic tools of inflicting costs on other states while avoiding full-blown conventional warfare render it politically infeasible for states to agree on the applicable rules for cyberspace. The fraught political difficulties of an international cyber treaty is evident from how the United States, Russia, and China refused to sign the 2018 Paris Call for Trust and Security in Cyberspace. It is a *non-binding* declaration that did not stipulate any substantive rules, but merely expressed a "willingness to work together, in the existing fora and through the relevant organizations, institutions, mechanisms and processes to assist one another and implement cooperative measures" in cyberspace.[114] Therefore, geopolitical realities problematize the possibility of states agreeing on an international cyber treaty.

Nevertheless, a treaty is neither the only nor most effective way of regulating cyberspace. Through monitoring and investigative reports, a fact-finding body can contribute to the gradual and cumulative crystallization of legal

[112] Mette Eilstrup-Sangiovanni, 'Why the World Needs an International Cyberwar Convention' (2017) 31 Philosophy and Technology 381.
[113] Valentin Jeutner, 'The Digital Geneva Convention' (2019) 10 Journal of International Humanitarian Legal Studies 160.
[114] Paris Call for Trust and Security in Cyberspace, 12 November 2018.

norms with respect to cyber operations as well as the stigmatization of cyber operations. Without informational transparency, stigma and norms cannot take root. In this proposal, however, investigative reports are not the only way in which legal ambiguity is reduced. The other complementary way is how victim and non-victim states react to these reports. As previously proposed, the body will not have enforcement powers with respect to its reports. The body only investigates and publishes the report; it leaves the decision of whether to respond and how to respond to victim and non-victim states. The reactions of victim and responsible states as well as neutral states to these reports can contribute to the gradual illumination, if not consolidation, of state practice and *opinio juris* on particular uses and conduct of cyber operations. At the very least, state responses to the body's investigative reports offer a window into how different states approach and conceptualize the use and conduct cyber operations. After all, one crucial obstacle to finding regulatory solutions in emerging international issues such as those in the cyber domain is the relative absence of information on state practice. Therefore, an international cyber treaty or the granting of enforcement powers is neither the only nor most effective way to address existing theoretical limits of international law in regulating cyber operations. The proposal also implies that in situations of international legal indeterminacy, an analysis of *how* norms shape state behaviour and *how* international legal principles can be integrated as norms rather than codified as enforceable rules can go a long way in maintaining peace and security.

In conclusion, one prevailing approach to regulating the use and conduct of cyber operations is to theoretically extend existing international law to the cyber domain in the form of an international cyber treaty. This approach, however, faces geopolitical constraints and theoretical limitations. With respect to use of cyber operations, there are theoretical limits to prohibiting cyber operations as internationally wrongful acts of a state. With respect to conduct of cyber operations, the character of cyber warfare and the nature of societies in which cyber operations are conducted pose unique challenges to the applicability and effectiveness of IHL in constraining the destructive humanitarian effects of cyber operations. By stipulating rights and obligations, treaties are an intuitive legal mechanism for addressing international legal lacunas. Such a treaty-based approach is, however, likely ineffective not only because of realpolitik but also the theoretical limits of international law with respect to the cyber domain. Conversely, an independent fact-finding body can play an important facilitative

role in the development of norms in cyberspace. By gradually crystallizing and capitalizing on international legal norms, an independent fact-finding body can address the current limitations faced by international law in regulating the use and conduct of cyber operations.