NEW ZEALAND CENTRE FOR PUBLIC LAW
Te Wānanga o ngā Kaupapa Ture ā Iwi o Aotearoa

New Zealand Journal of Public and International Law

VOLUME 17 ▪ NUMBER 1 ▪ NOVEMBER 2019

SPECIAL CONFERENCE ISSUE: 26TH ANNUAL ANZSIL CONFERENCE
FROM THE LOCAL TO THE GLOBAL
SPECIAL ISSUE EDITOR: ALBERTO COSTI

THIS ISSUE INCLUDES CONTRIBUTIONS BY

Yao Dong
Dame Sian Elias
Rosie Fowler
Robert French AC
Emma Palmer
Stephen Eliot Smith

The Law Foundation NEW ZEALAND SUPPORTING INDEPENDENT LEGAL THINKING

Australian and New Zealand Society of International Law

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA UNIVERSITY OF WELLINGTON

NEW ZEALAND JOURNAL OF PUBLIC AND INTERNATIONAL LAW

Faculty of Law
Victoria University of Wellington
PO Box 600
Wellington
New Zealand

November 2019

The mode of citation of this journal is: (2019) 17 NZJPIL (page)

The previous issue of this journal was volume 16 number 1, November 2018

ISSN 1176-3930

Printed by City Print Communications, Wellington

Cover photo: Robert Cross, VUW ITS Image Services

CONTENTS

The **New Zealand Journal of Public and International Law** is a fully refereed journal published by the New Zealand Centre for Public Law at the Faculty of Law, Victoria University of Wellington. The Journal was established in 2003 as a forum for public and international legal scholarship. It is available in hard copy by subscription and is also available on the HeinOnline, Westlaw, Informit and EBSCO electronic databases.

NZJPIL welcomes the submission of articles, short essays and comments on current issues, and book reviews. Manuscripts and books for review should be sent to the address below. Manuscripts must be typed and accompanied by an electronic version in Microsoft Word or rich text format, and should include an abstract and a short statement of the author's current affiliations and any other relevant personal details. Manuscripts should generally not exceed 12,000 words. Shorter notes and comments are also welcome. Authors should see earlier issues of NZJPIL for indications as to style; for specific guidance, see the *New Zealand Law Style Guide* (3rd ed, 2018). Submissions whose content has been or will be published elsewhere will not be considered for publication. The Journal cannot return manuscripts.

Regular submissions are subject to a double-blind peer review process. In addition, NZJPIL occasionally publishes addresses and essays by significant public office holders. These are subject to a less formal review process.

Contributions to NZJPIL express the views of their authors and not the views of the Editorial Committee or the New Zealand Centre for Public Law. All enquiries concerning reproduction of the Journal or its contents should be sent to the Student Editor.

Annual subscription rates are NZ$100 (New Zealand) and NZ$130 (overseas). Back issues are available on request. To order in North America contact:

Gaunt Inc
Gaunt Building
3011 Gulf Drive
Holmes Beach
Florida 34217-2199
United States of America
e-mail info@gaunt.com
ph +1 941 778 5211
fax +1 941 778 5252

Address for all other communications:

The Student Editor
New Zealand Journal of Public and International Law
Faculty of Law
Victoria University of Wellington
PO Box 600
Wellington, New Zealand
e-mail nzjpil-editor@vuw.ac.nz
fax +64 4 463 6365

NEW ZEALAND JOURNAL OF PUBLIC AND INTERNATIONAL LAW

The New Zealand Centre for Public Law was established in 1996 by the Victoria University of Wellington Council with the funding assistance of the VUW Foundation. Its aims are to stimulate awareness of and interest in public law issues, to provide a forum for discussion of these issues and to foster and promote research in public law. To these ends, the Centre organises a year-round programme of conferences, public seminars and lectures, workshops, distinguished visitors and research projects. It also publishes a series of occasional papers.

Directors

Director	*Associate Professor Joel Colón-Ríos*
Associate Director	*Dr Guy Fiti Sinclair*
Events and Centres Coordinator	*Ms Sharelle Kooyman*

For further information on the Centre and its activities visit www.victoria.ac.nz/nzcpl or contact the Events and Centres Coordinator at nzcpl@vuw.ac.nz, ph +64 4 463 6327, fax +64 4 463 6365.

THE *JUS AD BELLUM* IN CYBERSPACE: WHERE ARE WE NOW AND WHAT NEXT?

Yao Dong*

Allegations of "cyber attacks" have become a common occurrence in the media and public discourse. Examples include the 2007 cyber operations against Estonia which caused massive social and economic disruption, similar cyber operations against Georgia in 2008, the Stuxnet operation which damaged Iranian nuclear facilities, and the alleged Russian hacking into the United States Democratic National Committee computer network among numerous other targets. Such incidents have led to analyses of whether and how existing international law principles apply to cyber warfare. The most notable works are the Tallinn Manual on the International Law Applicable to Cyber Warfare *and the* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *This article provides an updated discussion and critique on the* jus ad bellum *(the international law governing the use of force) in the cyber context, and goes on to make recommendations for the* jus ad bellum *to better adapt to the new effects and capacities of cyber operations.*

I INTRODUCTION

It is easy to believe that the internet's transnational character makes it inherently unable to be regulated. But much of the scholarship on international law in the cyber context takes the view that existing international law principles govern cyberspace, despite difficulties in their application, and this is now mostly settled. In 2013, 20 senior international law practitioners and scholars, known as the International Group of Experts, produced the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (*Tallinn Manual*), a manual on how existing international law principles apply to cyber warfare.[1] While the *Tallinn Manual* demonstrates how existing international law principles may work, scholars have raised doubts about the applicability of international law to cyberspace, both before and certainly after its publication. Even those who are confident that international law applies

* BA/LLB(Hons). This article is a modified version of a paper submitted as part of the LLB(Hons) programme at the University of Auckland in October 2018. I would like to thank John Ip for his support and guidance.

1 Michael N Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, New York, 2013) [*Tallinn Manual*].

to cyberspace acknowledge that cyber operations often do not fit easily into the existing legal regimes.[2]

In this article, I argue that existing international law principles provide a useful basis to develop rules specific to cyberspace, which are required for a more accurate, effective and complete regulatory response. In making this argument, I focus on the *jus ad bellum*, a regime of international law which governs when force may be used. Part II examines key issues in the *jus ad bellum* and applies current principles, drawing mostly upon the *Tallinn Manual*, but also inserting recent examples and other legal analyses, including the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (*Tallinn Manual 2.0*), where it differs from the original.[3] Part III evaluates how well the *jus ad bellum* regulates when and how states may conduct cyber warfare, and considers how international law may develop to ameliorate the difficulties of applying the *jus ad bellum* in the cyber context. The conclusion sets out the two most pertinent issues hindering the accuracy, effectiveness and completeness of the *jus ad bellum* in the cyber context: the definition of cyber use of force and cyber armed attack; and attribution. I especially recommend two changes to the *jus ad bellum* so that both physical and non-physical effects may be considered when determining whether there has been a cyber use of force, and so that there is recourse to international law for wrongful acts in cyberspace.

I am mindful of terminology because of the legal consequences of classifying certain conduct as an intervention, use of force or armed attack. I am also aware of the common usage of the term "cyber attack" in the media and public discourse. In light of this, I will use the term "cyber operation" in a broad sense to refer to any "employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace".[4] Other terms will be defined as necessary throughout the article.

II THE APPLICABILITY OF THE JUS AD BELLUM *IN CYBERSPACE*

The *jus ad bellum* mainly developed after the Second World War, and prohibits the use of force except when authorised under Chapter VII of the Charter of the United Nations (UN) or in self-defence. Despite being a set of legal boundaries drawn in the context of conventional warfare, the *jus ad bellum* is widely assumed to apply to cyber warfare, usually by analogy to conventional warfare, in the sense that the effects of cyber operations are compared to those of non-cyber operations in

---

2 Christopher S Yoo "Cyber Espionage or Cyberwar?" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 175 at 176; and Duncan Hollis "Re-Thinking the Boundaries of Law in Cyberspace" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 129 at 129–131.

3 Michael N Schmitt (ed) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, New York, 2017) [*Tallinn Manual 2.0*].

4 *Tallinn Manual*, above n 1, at 258.

determining what is a use of force and an armed attack. The *Tallinn Manual* is premised upon the applicability of the *jus ad bellum* (and the *jus in bello*) to cyber operations.[5] This was the unanimous view of the International Group of Experts invited by the NATO Cooperative Cyber Defence Centre of Excellence to examine the law governing cyber warfare.[6] Furthermore, a number of states have accepted that existing international law principles apply in cyberspace, including the United States of America, the United Kingdom, Russia and China.[7]

From a normative perspective, the application of the *jus ad bellum* to cyber warfare is desirable because it appeals to the goal of ensuring that cyberspace does not become a legal loophole.[8] If cyber warfare were not subject to the *jus ad bellum* and were given sui generis treatment, then it would be effectively unregulated, in light of the general principle that acts not prohibited under international law are permitted.[9] To the extent that cyber operations have effects analogous to those effects which do not constitute a use of force in conventional warfare, it would make sense to also reject those cyber operations as a use of force.[10]

The starting point of the *jus ad bellum* is the UN Charter. Article 2(4) of the UN Charter prohibits the use of force against other states:

> All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

The UN Charter recognises two exceptions to the prohibition on the use of force: Chapter VII authorisation; and self-defence.[11] Article 51 of the UN Charter preserves:

---

5 At 5.

6 The International Group of Experts based their view on *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226 [*Nuclear Weapons*] at [39], where the International Court of Justice held that the *jus ad bellum* governs "any use of force, regardless of the weapons employed".

7 The President of the United States *International Strategy for Cyberspace* (The White House, May 2011); Harold Koh, Legal Adviser of the United States Department of State "International Law in Cyberspace" (USCYBERCOM Inter-Agency Legal Conference on the Roles of Cyber in National Defense, Fort Meade, Maryland, 18 September 2012); Brian J Egan "International Law and Stability in Cyberspace (2017) 35 Berkeley J Intl Law 169; Jeremy Wright, Attorney General of the United Kingdom "Cyber and International Law in the 21st Century" (Chatham House Royal Institute for International Affairs, 23 May 2018); and United Nations Group of Governmental Experts *Report on Developments in the Field of Information and Telecommunications in the Context of International Security* A/68/98 (2013).

8 Hollis, above n 2, at 149.

9 *SS "Lotus" (France v Turkey) (Judgment)* (1927) PCIJ (series A) No 10 at 19.

10 Hollis, above n 2, at 150.

11 Chapter VII authorisation is not discussed as it is a political process and is outside the scope of this article.

> … the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security.

While the UN Charter is not the only source of the *jus ad bellum*, the International Court of Justice has recognised that rules on the prohibition on the use of force and the right of self-defence in the UN Charter are part of customary international law.[12]

A Use of Force

There is no definition of the use of force in the UN Charter, nor is there an authoritative definition in other treaties. Some guidance may be drawn from the *travaux préparatoires* of art 2(4), which reveal that the negotiating states considered and rejected a proposed amendment to include economic coercion as a use of force.[13] The General Assembly also rejected an argument that political and economic forms of pressure fell within the scope of a use of force in the course of adopting the Declaration on Friendly Relations.[14] Furthermore, in *Military and Paramilitary Activities*, the International Court of Justice held that the funding of guerrilla operations against another state was not a use of force. These precedents led the International Group of Experts to conclude that:[15]

> … non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy do not qualify as uses of force … [and] merely funding a hacktivist group conducting cyber operations as part of an insurgency would not be a use of force.

However, in *Military and Paramilitary Activities*, the International Court of Justice also found that arming and training guerrillas who are engaged in operations against another state would be a use of force.[16] This means that a use of force need not be a direct use of armed force. Accordingly, providing an organised group with malware and training to carry out a cyber operation against another state would appear to constitute a use of force.[17]

---

12 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits)* [1986] ICJ Rep 14 [*Military and Paramilitary Activities*] at [188]–[190] and [193].

13 *Summary Report of Eleventh Meeting of Committee I/1* UN Doc 784 (5 June 1945) at 4; *Documentation for Meetings of Committee I/1* UN Doc 215 (11 May 1945) at 27–28; and *Addition to Chapter XII submitted by the Brazilian Delegation* UN Doc 2 G/7(e)(4) (6 May 1945) at 2–3.

14 *Special Committee on Principles of International Law concerning Friendly Relations and Co-operation among States* A/AC.125/SR.110 to 114 (1970); and *Report of the Special Committee on Friendly Relations and Co-operation among States* A/7326 (1969).

15 *Tallinn Manual*, above n 1, at 46.

16 *Military and Paramilitary Activities*, above n 12, at [228].

17 *Tallinn Manual*, above n 1, at 46.

Although these guides indicate that non-destructive operations with the sole intent of political or economic coercion are not uses of force, and the mere funding of a hacktivist group (independent groups with political and ideological motivations) is not a use of force, the determination of whether a cyber operation rises to the level of a use of force remains an uncertain task. The *Tallinn Manual* describes a general rule: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[18] However, in the absence of an authoritative definition of use of force outside the cyber context, it is hard to define which cyber operations qualify as uses of force, especially when cyber technology may quickly outdate previous understandings of the *jus ad bellum*.

The *Tallinn Manual* identifies the most aggressive cyber operations which clearly amount to uses of force, and lists eight non-exclusive factors to guide the inquiry in other cases. Cyber operations which "injure or kill persons or damage or destroy objects" are unambiguously uses of force.[19] In less obvious situations, states are likely to consider the factors of severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality.[20] Although severity is the most significant factor, the weight attributed to the various factors depends on the context in which the cyber operation occurs. For example, even though economic coercion is presumptively lawful, highly invasive cyber operations which cripple the target state's economy may nevertheless constitute a use of force.[21]

The United States of America and the United Kingdom have suggested a number of hypothetical examples of a cyber operation amounting to a use of force: the triggering of a nuclear plant meltdown resulting in widespread loss of life; the opening of a dam above a populated area causing destruction, the disabling of an air traffic control system with the effect of downing civilian aircraft; and the targeting of an essential medical service.[22] Meanwhile, according to the International Group of Experts, there is one actual example of a cyber use of force: the Stuxnet operation against Iranian nuclear centrifuges which was discovered in 2010, many months after the system was infected.[23] This

18 At 45.

19 At 48.

20 At 48–51.

21 At 52.

22 Koh, above n 7; and Wright, above n 7.

23 *Tallinn Manual*, above n 1, at 45.

involved malware which affected the control of centrifuges associated with an Iranian nuclear programme, causing damage to 1,000 centrifuges which required repairs.[24]

The analysis and the examples show that the threshold of the use of force is high and leaves most cyber operations, such as surveillance and temporary denials of service, outside the scope of the *jus ad bellum.* But cyber operations that do not rise to the level of a use of force may still be prohibited under international law by the principle of non-intervention, which imposes a duty not to interfere with the internal and external affairs of another state.[25] The principle of non-intervention is implicit in the principle of sovereign equality expressed in art 2(1) of the UN Charter. Although what constitutes intervention is heavily debated, the International Court of Justice has recognised that coercion on political, economic, social and cultural matters would amount to intervention.[26] So, for example, while the funding of guerrilla operations against another state is not a use of force, it is "undoubtedly an act of intervention" in the state's internal affairs.[27]

Still, not all cyber operations against another state automatically amount to intervention which is prohibited. Cyber operations which lack a coercive element do not breach the principle of non-intervention per se.[28] Instead, there is a broad spectrum of cyber operations which span a continuum from information gathering at one end to cyber crime and cyber espionage, which are almost entirely governed under domestic law, to cyber intervention, cyber armed attack and cyber warfare, at the other end.[29] For example, the 2007 cyber operations against Estonia, which rendered targeted governmental and media websites inaccessible for periods of time, probably did not reach the threshold to engage the principle of non-intervention or the *jus in bellum*, even if attribution of the cyber operations to a particular state were possible.[30] Likewise, the recent allegations of Russian hacking into the United States Democratic National Committee computer network, World Anti-Doping Agency, Organisation for the Prohibition on Chemical Weapons and numerous other targets

---

24 William H Boothby "Deception in the Modern, Cyber Battlespace" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 195 at 198; and Hollis, above n 2, at 149.

25 *Military and Paramilitary Activities in Nicaragua*, above n 12, at [205].

26 At [205].

27 At [228].

28 *Tallinn Manual*, above n 1, at 44.

29 At 4; Laurie R Blank "Cyberwar versus Cyber Attack" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 76 at 78; and Yoo, above n 2, at 188–190.

30 Boothby, above n 24, at 197–198.

are unlikely to amount to interventions, let alone uses of force, because the element of coercion does not appear to be present.[31]

B Attribution

Article 2(4) of the UN Charter only applies to uses of force which are conducted by states or are otherwise attributable to states.[32] The International Law Commission's Articles on State Responsibility largely codify the customary international law of state responsibility.[33] An act or omission shall be attributed to a state if the actor is an organ of that state under art 4, if the actor is exercising government authority under art 5, or if the actor is acting on the instructions, or under the direction or control, of that state under art 8.

Attribution raises unique technical and legal challenges in the cyber context. At first, an actor may mask their IP address using obfuscation techniques.[34] Even if the location of the computer used to carry out the cyber operation were known, it does not definitively give away who was operating the computer. And even if the actor were identified, there would still be the obstacle of linking the actor to a state. The target state may need the assistance from the state in which the attack originated or passed through.[35]

The difficulty of determining and proving attribution is seen in the 2007 cyber operations against Estonia, which were never formally attributed to any state because the actors were believed to be patriotic hackers, who believed in defending the interests of their state, and whose relationship with the Russian government was never proved.[36] Estonia had submitted several requests for assistance in tracking the origin of the cyber operations to Russia, but the requests were rejected despite a bilateral legal assistance treaty.[37] When Georgia was the target of similar denial of service operations in 2008, it also struggled to attribute the conduct of patriotic hackers to the Russian government.[38]

---

31 "Russia cyber-plots: US, UK and Netherlands allege hacking" (4 October 2018) BBC News <www.bbc.com/news>; and Jens David Ohlin "Did Russian Cyber Interference in the 2016 Election Violate International Law?" (2017) 95 Tex L Rev 1579 at 1592-1593.

32 *Tallinn Manual*, above n 1, at 43.

33 *Responsibility of States for Internationally Lawful Acts* GA Res 56/83, A/Res/56/83 (2001), annex [Draft Articles].

34 Luke Chircop "A Due Diligence Standard of Attribution in Cyberspace" (2018) 67 ICLQ 643 at 646.

35 Nicolò Bussolati "The Rise of Non-State Actors in Cyberwarfare" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 102 at 121.

36 At 111.

37 At 121.

38 Boothby, above n 24, at 198.

Recognising the difficulty of attribution in the cyber context, the *Tallinn Manual* sets out two rules which are not particularly helpful to the task of attribution. Rule 7 provides:[39]

> The mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State, but is an indication that the State in question is associated with the operation.

Rule 8 states: "The fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State."[40]

The Estonian and Georgian examples illustrate a further challenge for attribution in the cyber context: the prevalence of non-state actors. The *Tallinn Manual* observes that the prohibition on the use of force only applies to the conduct of non-state actors if the conduct is attributable to a state.[41] The law of state responsibility allows the conduct of non-state actors to be attributed to a state in limited circumstances. Article 8 of the Articles on State Responsibility is particularly relevant: it provides for attribution where the non-state actor is acting on the instructions, or under the direction or control, of the state.[42]

The International Court of Justice considers the criterion of control to be a standard of "effective control" in respect of each operation, rather than in respect of the overall actions.[43] A lesser standard of "overall control" was adopted by the International Criminal Tribunal for the Former Yugoslavia (ICTY) Appeals Chamber in *Tadić*.[44] However, the International Court of Justice in the *Genocide case* distinguished *Tadić* on the basis that the ICTY Appeals Chamber was not dealing with an issue of state responsibility, which would be outside its jurisdiction.[45] The Court also observed that:[46]

> ... the "overall control" test has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf.

---

39 *Tallinn Manual*, above n 1, at 34.

40 At 36.

41 At 43-44.

42 Draft Articles, above n 33, art 8.

43 *Military and Paramilitary Activities*, above n 12, at [115]; and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 43 [*Genocide*] at [399]-[401].

44 *Prosecutor v Tadić (Judgment)* ICTY Appeals Chamber IT-94-1-A, 15 July 1999 [*Tadić*], at [131] and [145].

45 *Genocide*, above n 43, at [403]-[405].

46 At [406].

Even if the overall control test were applied, the degree of control required to attribute the conduct of a non-state actor to a state would need to be more than the mere funding or equipping of the non-state actor.[47] Furthermore, the ICTY Appeals Chamber restricted the overall control test to groups with a degree of organisation and hierarchical structure, as opposed to individuals and unorganised groups who were subject to the effective control test.[48] Hacktivist groups and patriotic hacker groups tend to have an informal structure.[49] Large hacker groups might be arranged in a two-tiered structure consisting of administrators at the top and affiliated users at the bottom.[50] Even then, the degree of affiliation between the users and the administrators may vary, and the decision to take action may be made by individual users who may be influenced by different shades of motivations. For a state to have overall control of the group, it would need to have a tight connection with or be part of the administrative level of the group, and issue instructions which filter through to all of the affiliated users.[51] The effective control test is even harder to meet, given that it requires specific directions about each operation and hacker groups often cannot control individual users' actions.

Therefore, most non-state actors would fall outside the scope of the law of state responsibility, and enjoy "a relative degree of impunity from the harmful consequences of their conduct".[52] Attribution of the conduct of a non-state actor to a state is required to assess the legal consequences of the conduct, such as the target state's right of self-defence. However, in the context of international terrorism, evolving state practice has supported an interpretation of art 51 of the UN Charter which pushes the scope of the right of self-defence beyond the limits of the rules of attribution.[53] This will be discussed in the next section.

C Self-defence

The condition precedent for the exercise of the inherent right of self-defence preserved in art 51 of the UN Charter is the existence of an "armed attack". Armed attack is not defined in the UN Charter. The prevailing view is that an armed attack is a subset of the use of force – the two terms are not the same and give rise to different legal consequences. The International Court of Justice in *Military and Paramilitary Activities* distinguished between "the most grave forms of the use of force (those constituting an armed attack) [and] other less grave forms".[54] Therefore, it is possible for a state to be

47 *Tadić*, above n 44, at [145].

48 At [132].

49 Bussolati, above n 35, at 116.

50 At 117.

51 At 120.

52 Chircop, above n 34, at 647.

53 Bussolati, above n 35, at 122.

54 *Military and Paramilitary Activities*, above n 12, at [191].

the target of conduct which rises to the level of a use of force prohibited under art 2(4), but does not rise to the level of an armed attack and thus does not trigger a right of self-defence. In other words, armed attack is a higher threshold. The determination of an armed attack depends on its "scale and effects".[55] This says nothing about a number of further issues, such as whether physical injury or damage is required, and the treatment of pinprick operations and non-state actors.

Notably, the United States of America denies that there is a gap between a use of force and an armed attack. The Legal Adviser of the Department of State confirmed the United States' view in 2012:[56]

> … the inherent right of self-defense potentially applies against *any* illegal use of force. In our view, there is no threshold for a use of deadly force to qualify as an "armed attack" that may warrant a forcible response.

None of the International Group of Experts agreed with this position.[57] It widens the scope of when a target state is allowed to respond with its own use of force. The danger is that it relaxes the criteria for the exercise of the right of self-defence, relying upon the customary international law requirements of necessity and proportionality to maintain international peace and security.

A narrow interpretation of "armed attack" would restrict its meaning to kinetic armed attacks, which would exclude cyber operations.[58] But this would be inconsistent with the treatment of chemical, biological and radiological attacks as being capable of triggering the right of self-defence, despite their non-kinetic nature.[59] Therefore, the view that cyber operations may never amount to an armed attack is generally rejected.[60] A notable exception is China, which has resisted the idea that cyber operations may give rise to a right of self-defence and, alongside Russia, has advocated for a new convention to regulate cyber operations.[61] Still, in applying the rules of self-defence to cyberspace, "the International Group of Experts unanimously concluded that some cyber operations

---

55 At [195].

56 Koh, above n 7.

57 Michael N Schmitt "The Use of Cyber Force and International Law" in Marc Weller (ed) *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, Oxford, 2015) 1110 at 1119.

58 Matthew C Waxman "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions" (2013) 89 Intl L Stud 109 at 111.

59 *Tallinn Manual*, above n 1, at 54.

60 Waxman, above n 58, at 111.

61 At 115.

may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter."[62]

The critical factor of a cyber armed attack is whether the effects are sufficiently similar to those of a kinetic armed attack.[63] Recalling that the International Court of Justice characterised armed attacks as "the most grave forms of the use of force", the International Group of Experts agreed that a cyber operation would clearly amount to an armed attack if it "injures or kills persons or damages or destroys property".[64] But cyber intelligence gathering, cyber theft and brief or period interruption of non-essential cyber services would not constitute armed attacks. From a political perspective, a cyber armed attack is likely to require a higher threshold of harm than a kinetic armed attack, because cyber operations are often covert and invisible to the public, and the perpetrator is often difficult to prove to domestic and international audiences.[65] Thus, states would struggle to gain support from their citizens and other states for forcible responses to cyber armed attacks which do not have significant and publicly perceptible effects.

It remains uncertain whether cyber operations not resulting in injury, death, damage or destruction may amount to an armed attack. The International Group of Experts were divided on this question: some members thought that physical injury or damage to persons or property was a requirement, while other members focused on the severity rather than the nature of the effects.[66] The paradigmatic case which illustrates this division of opinion is a cyber operation against a major international stock exchange, causing the market to crash. On the former, narrower view, the taking down of the stock market would not constitute an armed attack. On the latter, broader view, the catastrophic effects of a stock market crash would be sufficient for the cyber operation to constitute an armed attack.

If cyber operations not resulting in physical injury or damage may never be an armed attack, a seemingly odd consequence would be that a cyber operation which opens a dam and floods several houses would qualify as an armed attack, while a cyber operation that crashes a stock market would not.[67] Common sense would indicate that the flooding of several houses is less serious than the crashing of a stock market. Those of a broader, effects-based view argue that that to focus on physical

62 *Tallinn Manual*, above n 1, at 54.

63 Waxman, above n 58, at 111.

64 *Tallinn Manual*, above n 1, at 55.

65 Waxman, above n 58, at 119–120.

66 *Tallinn Manual*, above n 1, at 56.

67 Schmitt, above n 57, at 1120.

injury or damage fails to account for the modern state's critical dependence on information infrastructure and connectivity.[68]

The massive social and economic disruption suffered by Estonia in 2007 demonstrates this concern. The cyber operations seriously impaired the daily operation of Estonian banks, government departments and businesses, and resulted in losses estimated at USD 27 to 40 million.[69] In 2012, the United Kingdom Minister for the Armed Forces said that cyber operations like those suffered by Estonia might trigger NATO's collective self-defence provisions.[70] This suggests a lean towards the effects-based approach to armed attack.

The effects-based approach leads to an issue about which effects may be included in assessing whether a cyber operation constitutes an armed attack. This is a causation problem. The International Group of Experts adopted a proximate cause standard, which means that the consequences of a cyber operation must be reasonably foreseeable to give rise to a right of self-defence.[71] The proximate cause standard runs into difficulties when considering the case of the stock market crash. Imagine that a wave of cyber operations causes a stock market crash, which destabilises the economy and produces widespread unemployment; a second wave of cyber operations causes wide fluctuations in the state's currency; and a third wave of cyber operations breaches the security of banks and causes widespread panic in the population, which triggers price gouging, looting and riots. The question that the proximate cause standard does not answer is whether the acts of intervening human agents – the price gougers, looters and rioters – break the chain of causation.[72]

A potential solution is to develop a bright line rule. For example, states may agree in a future convention that all intended consequences, regardless of the acts of intervening human agents, shall have a sufficient causal link to the original cyber operation.[73] A bright line rule may be arbitrary, but may appeal in the context of self-defence because a target state must determine for itself whether an armed attack has occurred and whether self-defence is justified, and the rest of the world must evaluate the legality of any forcible response based on the available intelligence.[74] However, a multilateral

---

68 Waxman, above n 58, at 112.

69 Samuli Haataja "The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach" (2017) 9 LIT 159 at 161.

70 "UK minister: Cyberattack could prompt NATO action" *The Seattle Times* (online ed, Seattle, 17 May 2012).

71 *Tallinn Manual*, above n 1, at 57; and Jens David Ohlin "Cyber Causation" in Jens David Ohlin, Kevin Govern and Claire Finkelstein (eds) *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, Oxford, 2015) 37 at 45.

72 Ohlin, above n 71, at 46.

73 At 53.

74 At 50.

treaty which answers legal questions about cyber operations as armed attacks is unlikely to eventuate as states are divided in their views on how cyberspace should be regulated.[75]

Another issue which is particularly relevant in the cyber context is whether the effects of pinprick cyber operations which do not individually rise to the level of armed attack may be combined to amount to an armed attack. The International Group of Experts took the position that pinprick cyber operations may be treated as a composite armed attack if they are launched by a single originator or originators acting in concert.[76] The cyber operations must be sufficiently related to be considered as "constituent parts of a single broader campaign".[77] This is consistent with the *Oil Platforms* case, in which the International Court of Justice entertained the prospect that a series of smaller operations might constitute an armed attack when combined.[78]

When it comes to non-state actors, state practice following 9/11 appears to support an interpretation of art 51 of the UN Charter which does not require attributing the conduct of a non-state actor to a state. This interpretation is possible because while art 2(4) prohibits members of the UN from the use of force, art 51 does not stipulate who the originator of an armed attack must be. Although the International Court of Justice has suggested a restrictive approach which limits the right of self-defence to cases of armed attack by one *state* against another state, in two post 9/11 decisions, a handful of states have used force directly against non-state actors in reliance on the right of self-defence, and a considerable number of states have supported it.[79]

For example, on 7 October 2001, the United States of America and the United Kingdom reported to the UN Security Council that their armed forces had commenced actions in Afghanistan, in response to the 9/11 attacks and in exercise of individual and collective self-defence.[80] The actions were directed against Al Qaeda, which was responsible for the attacks, and the Taliban regime, which

---

75 Adam Segal and Matthew Waxman "Why a cybersecurity treaty is a pipe dream" (27 October 2011) The Global Public Square <http://globalpublicsquare.blogs.cnn.com>; and Arun M Sukumar "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?" (4 July 2017) Lawfare <www.lawfareblog.com>.

76 *Tallinn Manual*, above n 1, at 56.

77 Schmitt, above n 57, at 1121.

78 *Oil Platforms (Islamic Republic of Iran v United States of America) (Merits)* [2003] ICJ Rep 161 at [64].

79 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136 at [139]; and *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment)* [2005] ICJ Rep 168 at [146]–[147].

80 Letter from John Negroponte (Permanent Representative of the United States to the United Nations) to the President of the Security Council regarding the initiation of actions in self-defence following the 9/11 attacks (7 October 2001); and Letter from Stewart Eldon (Chargé d'Affaires of the Permanent Mission of the United Kingdom to the United Nations) to the President of the Security Council regarding the initiation of actions in self-defence following the 9/11 attacks (7 October 2001).

was accused of tolerating and harbouring Al Qaeda. Many states endorsed the actions: NATO and the Organization of American States invoked the collective defence provisions under their respective treaties, and individual states such as Australia took the position that the actions were an exercise of collective self-defence.[81] In addition, the Security Council had earlier adopted Resolutions 1368 and 1373, which seemed to accept and confirm that the right of self-defence was applicable to the 9/11 attacks, without attributing the conduct to a state.[82]

On this basis, the majority of the International Group of Experts concluded that there is a right of self-defence in response to cyber armed attacks by non-state actors.[83] The right of self-defence does not only pertain to cyber operations by terrorist or rebel groups, but also private commercial entities such as IT companies or internet service providers. However, the majority of the International Group of Experts split over whether some degree of organisation is required in a non-state actor to be able to mount an armed attack. Michael Schmitt was among the members who took the view that the right of self-defence never applies to unorganised non-state groups or individuals.[84] This position would rule out many cyber operations such as those against Estonia and Georgia in 2007 and 2008, during which individuals decided to act alone or responded to a general call to launch attacks.

The problem with a right of self-defence against non-state actors is that a forcible response must be taken against the state in which the non-state actor is located, even if the host state was not involved in the armed attack, unless the host state gives its consent. States and scholars have suggested a number of legal theories to legitimise the use of defensive force against the host state. State practice has approved the use of force in self-defence against non-state groups in the host state if the host state is unwilling or unable to suppress the threat of the non-state actor.[85] This was the legal basis for, inter alia, Russia's use of force against the Chechen rebels in Georgia, and the United States and Israel's use of force against Hezbollah in Lebanon. The idea of the unwilling or unable test is not new – it traces back to the *Caroline* case of 1837.[86] The majority of the International Group of Experts concluded that self-defence in response to a cyber armed attack by a non-state actor is permissible if the unwilling or unable criterion is satisfied.[87] However, this does not explain why the host state must accept an infringement of its sovereignty.

---

81 Schmitt, above n 57, at 1122.

82 SC Res 1368, S/Res/1368 (2001); and SC Res 1373, S/Res/1373 (2001).

83 *Tallinn Manual*, above n 1, at 59.

84 Schmitt, above n 57, at 1123.

85 Bussolati, above n 35, at 123.

86 Ashley S Deeks "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense" (2012) 52 Va J Intl L 483 at 502.

87 *Tallinn Manual*, above n 1, at 60–61.

Other legal grounds advanced for the extension of the right of self-defence to cover self-defence against non-state actors include the right of self-preservation of the target state, an *erga omnes* obligation to defend the values represented in the fight against international terrorism, and the host state's obligation not to knowingly allow acts contrary to the rights of other states to be carried out from its territory.[88] In the cyber context, the obligation not to tolerate or harbour non-state actors may extend to multiple host states because hacker groups may be composed by members or may use servers located in multiple jurisdictions. This may entail the expansion of the obligation to cover the provision of a virtual shelter to a hacker group. Thus, host states may have an increased duty to control their IT systems.

The expansion of the right of self-defence to non-state actors is an unsettled area of international law, especially in the cyber context. It has the potential to overcome the difficulty of attributing cyber operations to a state according to the law of state responsibility and augment the ability of the target state to prevent further armed attacks. However, it may also increase the risk of states reacting impulsively with force to cyber armed attacks without analysing sufficiently the origin of the attack, the unwillingness or inability of the host state to suppress the threat, or the connivance of the host state.[89]

Once an armed attack has triggered a right of self-defence, the exercise of the right of self-defence is subject to the customary international law requirements of necessity and proportionality.[90] A use of force in self-defence must be necessary to prevent or defeat an armed attack which is underway or imminent.[91] Where other, non-forcible responses are available, such other responses must be insufficient to address the threat. If defensive force is deemed necessary, the proportionality criterion limits its scale, scope, duration and intensity to the extent required to prevent or defeat the armed attack which is underway or imminent.[92] The level of force used in self-defence may exceed the level of force employed in the original armed attack which triggered the right of self-defence, as long as it is no more than necessary to prevent or defeat a further armed attack.

In the cyber context, the effects of defensive use of force may bleed over into systems unconnected with the original or further armed attack. According to Schmitt, the defensive use of force is not necessarily prohibited by the proportionality criterion if the bleed-over effects are unavoidable.[93]

---

88 Bussolati, above n 35, at 123–124.

89 At 125.

90 *Military and Paramilitary Activities*, above n 12, at [176] and [194]; *Nuclear Weapons*, above n 6, at [41]; and *Oil Platforms*, above n 78, at [43], [74] and [76].

91 *Tallinn Manual*, above n 1, at 62.

92 At 62.

93 Schmitt, above n 57, at 1125.

However, if the bleed-over effects are suffered in a third, innocent state and the bleed-over effects amount to an armed attack, then the third state would have a right of self-defence.[94]

A final issue which plagues the exercise of the right of self-defence is its temporal limitations. Article 51 of the UN Charter refers to a right of self-defence arising upon the occurrence of an armed attack. This clearly covers an armed attack which has fully or partially materialised. For example, a cyber operation may be the first step of an armed attack, employed to disable the target's air defence system before a military strike.[95] This is likely what happened before the bombing of a Syrian nuclear reactor in 2007.[96] Israel only admitted the bombing earlier this year.[97] But attribution problems aside, the cyber operation alone would have been sufficient to trigger a right of self-defence for Syria because it facilitated the military strike and the overall armed attack.[98]

A more difficult scenario is when an armed attack is anticipated, but has not been launched. The *Caroline* case articulated a now well-recognised idea that self-defence may be exercised if an armed attack is "imminent", which meant "instant, overwhelming, leaving no choice of means, and no moment for deliberation".[99] The International Group of Experts accepted the idea of imminence.[100] However, the majority departed from the *Caroline* formulation of imminence, which imposed a strict temporal limit, requiring that an armed attack be about to be launched. They adopted the "last window of opportunity" standard, which defines imminence as a situation in which the target state "will lose its opportunity to effectively defend itself unless it acts".[101]

The last window of opportunity standard is not a concrete development in customary international law, although it echoes the idea of continuing imminence which has been advocated by the United Kingdom in the context of international terrorism. The United Kingdom sees imminence as a finding to be made in light of all relevant circumstances of each case, including:[102]

---

94 *Tallinn Manual*, above n 1, at 57.

95 At 63.

96 Adeo Fraser "From the Kalashnikov to the Keyboard: International Law's Failure to Define a 'Cyber Use of Force' is Dangerous and May Lead to a Military Response to a 'Cyber Use of Force'" (2016) 15 Hibernian LJ 86 at 98.

97 "Israel confirms bombing 'Syria nuclear reactor' in 2007" (21 March 2018) Al Jazeera <www.aljazeera.com>.

98 Fraser, above n 96, at 98; and Schmitt, above n 57, at 1126.

99 Letter from Daniel Webster (United States Secretary of State) to Lord Ashburton regarding the *Caroline* case (6 August 1842).

100 *Tallinn Manual*, above n 1, at 63.

101 At 63.

102 Arabella Lang *Legal basis for UK military action in Syria* (House of Commons, Briefing Paper 7404, 1 December 2015) at 16.

> … (a) the nature and immediacy of the threat, (b) the probability of an attack, (c) whether the anticipated attack is part of a concerted pattern of continuing armed activity, (d) the likely scale of the attack and the injury, loss, or damage likely to result therefrom in the absence of mitigating action, and (e) the likelihood that there will be other opportunities to undertake effective action in self-defence …

Still, there are other possible approaches to imminence, such as the United States' position of pre-emptive self-defence, which does not require an armed attack to be imminent at all.[103] However, this is not supported by other states. The International Group of Experts were clear that pre-emptive strikes are not a lawful exercise of the right of self-defence.[104]

In exercising the right of self-defence *after* an armed attack, the use of defensive force is subject to the principle of immediacy.[105] This means that the use of defensive force must be sufficiently proximate in time to the armed attack which triggered the right of self-defence to distinguish the use of defensive force from mere retaliation. Relevant factors may include the time elapsed between the armed attack and the response, the time required to identify the source of the armed attack, and the time required to prepare a response. In the cyber context, the immediacy criterion may preclude a number of defensive actions due to the target state not becoming aware that an armed attack has occurred for some time, either because the injury or damage is not immediately apparent or because the cause of the injury or damage is not identified until after the armed attack.[106] An example of such a situation is Stuxnet, which had created the impression that technical flaws in the system controlling the Iranian nuclear centrifuges caused the damage, rather than malware.

The analysis above shows that there are a few clear principles of self-defence which apply in the cyber context. A right of self-defence is triggered when an armed attack occurs. Armed attack is a higher threshold than use of force, distinguished by its scale and effects. A cyber operation may amount to an armed attack if its effects are sufficiently similar to those of a kinetic armed attack. And an exercise of force in self-defence is subject to the criteria of necessity and proportionality, and the principle of immediacy. However, numerous issues remain unresolved. Cyber operations not resulting in physical injury or damage may or may not be able to qualify as an armed attack. It is unclear what effects are too remote to be considered in assessing whether a cyber operation amounts to an armed attack. After 9/11, it seems that states may sometimes exercise a right of self-defence against a non-state actor, but the precise limits and basis for this are controversial. And finally, views on the extent

---

103 The President of the United States *The National Security Strategy of the United States of America* (The White House, September 2002) at 15.

104 *Tallinn Manual*, above n 1, at 65–66.

105 At 63.

106 At 66.

to which anticipatory self-defence is permitted vary between the *Caroline* case, states and the International Group of Experts.

III THE ADAPTABILITY OF THE JUS AD BELLUM *IN CYBERSPACE*

The position reflected in the *Tallinn Manual* is that a cyber use of force generally requires physical effects, such as injury to persons or damage to property, unless there are exceptional circumstances, such as a highly invasive cyber operation which cripples the target state's economy.[107] The test for a cyber use of force compares the cyber operation in question to non-cyber operations which would be considered uses of force.[108] Likewise, a cyber armed attack must have effects sufficiently similar to those of a kinetic armed attack. And it is likely that a cyber operation will *only* amount to an armed attack if it has physical effects.[109]

The inability of the *jus ad bellum* to recognise the harm caused by cyber operations with non-physical effects is illustrated by the 2007 cyber operations against Estonia. Although there was no injury, death, damage or destruction, the cyber operations severely disrupted government functions and services, and negatively impacted the economy and the daily lives of many people. However, the prevailing view is that the cyber operations against Estonia did not qualify as a use of force.[110] The *jus ad bellum* appears to be fixated on physical effects – it may be insufficient to govern cyber operations when their threat is to the welfare of a state which is critically dependent upon information infrastructure and connectivity.[111]

This is just one of numerous limitations of determining how an existing legal regime applies to cyber operations by analogy to how that regime applies to conventional warfare. It fails to address the expansion in the range of possible harm to states as cyber weapons are developed and as states are increasingly dependent on information systems.[112] The rationale behind analyses such as the *Tallinn Manual* is that the *jus ad bellum* ensures that cyberspace is not a law-free zone, while states remain unable to agree on a new legal regime to regulate cyberspace beyond the limited Convention on Cybercrime.[113] Analogical reasoning provides a useful foundation for delineating appropriate

---

107 At 52.

108 *Tallinn Manual*, above n 1, at 45.

109 Haataja, above n 69, at 172.

110 Boothby, above n 24, at 197–198; and Haataja, above n 69, at 173.

111 Waxman, above n 58, at 112.

112 Lucas Kello "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft" (2013) 38(2) International Security 7 at 21–37.

113 Hollis, above n 2, at 141 and 146; and Convention on Cybercrime 2375 UNTS 441 (opened for signature 23 November 2001, entered into force 1 July 2004).

boundaries of behaviour in cyberspace and legal boundaries offer a degree of certainty and constraint.[114] However, the theoretical and functional difficulties of applying the *jus ad bellum* in the cyber context require more thought, because they inform the direction in which international law is likely to develop as it responds to events.[115] They also have normative value as they inform how the *jus ad bellum* ought to develop, should the day that states are ready to create a new legal regime for cyberspace ever arrive. In analysing the theoretical and functional difficulties, Duncan Hollis' categories are particularly helpful.[116]

A Theoretical Difficulties

The extension of the *jus ad bellum* into cyberspace entails the division of cyberspace into territories governed by states, as the *jus ad bellum* only regulates inter-state uses of force. But international law also recognises non-territorial spaces, such as the high seas, which is under collective governance as *res communis*.[117] Territory and *res communis* are mutually exclusive notions. There is currently no unifying theory on the nature of cyberspace. The 2007 cyber operations against Estonia illustrate the legal implications that defining the nature of cyberspace may have: they crossed cyber infrastructure in over 100 states.[118] Therefore, any attempt to apply a legal regime which relies on territorial sovereignty, such as the *jus ad bellum*, forestalls a more fundamental question about what cyberspace is.[119]

Furthermore, the application of the *jus ad bellum* in the cyber context implicates the fragmentation of international law into a variety of defined areas with specialised rules, such as the law of the sea and human rights law. Analogical reasoning replicates existing fragmentation issues in cyberspace and generates new conflicts of law which did not previously arise.[120] For example, problems of attribution in the cyber context blur the line between criminal law, which regulates individuals, and the *jus ad bellum* and *jus in bello*, which regulates states. Therefore, cyberspace presents opportunities for new conflicts between legal regimes.[121]

---

114 Hollis, above n 2, at 155.

115 Fraser, above n 96, at 109.

116 Hollis, above n 2.

117 At 135–136.

118 Kello, above n 112, at 24.

119 Hollis, above n 2, at 136.

120 At 147–148.

121 At 148.

B Functional Difficulties

The application of the *jus ad bellum* to cyber warfare by relying on analogy, for example, to define cyber use of force and cyber armed attack, may be criticised on a number of functional grounds: accuracy; effectiveness; and completeness.[122] It is inaccurate because relevant differences between cyber operations and non-cyber operations are not considered when translating the *jus ad bellum* to cyberspace. The problems of attribution, especially the anonymity of cyber operations, make it difficult to ensure compliance with the law. As a result, the law is incomplete because it fails to accurately and effectively regulate cyberspace. These difficulties are discussed and some preferred alternatives are suggested below.

1 Accuracy

The definition of a cyber use of force by analogy to a non-cyber use of force may be both over-inclusive and under-inclusive, and thus inaccurate, due to relevant differences between the analogy's origin (conventional warfare) and its target (cyber warfare).[123] As demonstrated by the 2007 cyber operations against Estonia, the line drawn by analogy to non-cyber use of force leaves cyber operations with non-physical effects outside the *jus ad bellum*.[124] Cyber operations may have the objective of damaging the target computer system, such as Iranian nuclear centrifuges, or of hindering social, economic or government functions which rely on that computer system, such as Iran's ability to weaponise uranium.[125] The former, which has physical effects, may engage the *jus ad bellum* while the latter, which has non-physical but perhaps more powerful effects, may not. The point is that the threat to national security and the strategic purposes of states are subordinated in applying the *jus ad bellum* to cyberspace, with potentially interesting consequences for what may give rise to the right of self-defence. Defining a cyber use of force by reference to what would qualify as a use of force outside the cyber context may be under-inclusive, because it excludes any new effects which cyber operations may generate.[126] Conversely, defining what is a cyber use of force by reference to what would not qualify as a use of force outside the cyber context may be over-inclusive, because it would reflexively include any new cyber capacities.[127]

Another accuracy problem in applying the *jus ad bellum* in cyberspace is that a cyber operation is qualitatively different to a non-cyber operation. A weapon used in conventional warfare, including a nuclear weapon, must traverse some geographic space to cause direct material harm. In contrast, the

---

122 At 130.

123 At 148–149.

124 *Tallinn Manual*, above n 1, at 52; Boothby, above n 24, at 197–198; and Haataja, above n 69, at 173.

125 Kello, above 112, at 19–20.

126 Hollis, above n 2, at 150.

127 At 150.

nature of a cyber operation is an interruption or interference with electronic communications. Under art 41 of the UN Charter, this is not considered a use of armed force in the context of a Chapter VII authorisation.[128] Furthermore, the effects of a cyber operation would rarely be equivalent to those of a non-cyber operation. For example, the *Tallinn Manual* declares that Stuxnet amounted to a cyber use of force because of the damage it caused to 1,000 centrifuges.[129] But Stuxnet had achieved its result over the course of months, with no apparent harmful effects other than the damage to those centrifuges. A kinetic operation with the same objective as Stuxnet – incapacitating Iranian nuclear facilities – would have involved a heat blast from a military strike and collateral damage.[130] While the qualitative difference between cyber operations and non-cyber operations may seem like a lesser challenge than the new effects and capacities of cyber operations, it contributes to the more fundamental issue that cyber operations may lack a proximate cause of injury, yet may still cause great social and economic effects.[131]

A better approach to defining a cyber use of force is to craft a tailor-made line for cyberspace by assessing the new effects and capacities of cyber operations, in light of the purpose of maintaining international peace and security.[132] One possibility is to take an informational view of the harm caused by cyber operations, instead of fixating on physical effects pursuant to an anthropocentric and materialist view of harm.[133] This would improve the ability of the *jus ad bellum* to regulate cyberspace by reconceptualising what is violence which threatens the state. The informational view is concerned with the well-being of the infosphere, which includes the natural and digital environments. It sees all entities in terms of their informational structures, that is, the organisational structures of their institutions, and it supposes that all such informational entities have an inherent value.[134] This view may be more appropriate as states become increasingly dependent on their information systems and cyber operations become greater threats to their welfare.

From an informational perspective, the state is an entity into which information flows continuously from other entities and vice versa.[135] The state entity has both a physical presence within its territory and a virtual presence in cyberspace. It consists of informational structures bound to each

---

128 At 148–149.

129 *Tallinn Manual*, above n 1, at 45.

130 Hollis, above n 2, at 149.

131 Kello, above n 112, at 23–24.

132 Hollis, above n 2, at 150. See also Fraser, above n 96.

133 Haataja, above n 69, at 173.

134 At 175.

135 At 176.

other, and to the informational structures of other state entities, by a system of communication.[136] And it has a responsibility to protect both its natural and digital environments from entropy, which means degradation of being.[137] Accordingly, the harm caused by cyber operations may be rethought in terms of entropy as harm to the functioning of the state entity. Cyber operations such as those suffered by Estonia are hostile information flows which seek to disrupt or damage the ability of the state entity to function.[138] In this way, an informational view of the state and the notion of harm allows both physical and non-physical effects of cyber operations to be seen as harm to the state.

2 Effectiveness

Even if a cyber use of force were perfectly analogous to a non-cyber use of force, the result of applying the *jus ad bellum* in cyberspace by analogy may still be ineffective, because the existing legal regime is ill-suited to the technology it targets. The challenges of attribution in the cyber context make it difficult to ensure compliance with the law.[139] The *jus ad bellum* operates by proscription: it deters or remedies violations by permitting the target to use force in self-defence against the perpetrator. However, proscription requires attribution, which is hindered by the anonymity and uncertainty of cyber operations, and the accessibility of cyber weapons for non-state actors, whose conduct is sheltered by a relative degree of impunity.[140]

Not only is the perpetrator of a cyber operation hard to identify, the purpose of the cyber operation is also difficult to distinguish. The delayed discovery of Stuxnet shows that a state may mislabel cyber operations as computer error or equipment failure – the real cause of the damage was only found when an Iranian scientist unexpectedly connected his laptop to the device in which Stuxnet was squatting.[141] A state may also assume that a cyber operation is an act of crime rather than an act of war, leading to a different legal regime being applied.[142] Combining the anonymity and uncertainty of cyber operations with the prevalence of non-state actors and the nearly instantaneous speed at which cyber operations occur, the application of the *jus ad bellum* in cyberspace by analogy seems unlikely to effectively engender behaviour.[143] Arguably, it only provides grounds for debate ex post facto.

---

136 At 178.

137 At 176.

138 At 181.

139 Hollis, above n 2, at 151.

140 Chircop, above n 34, at 647.

141 Fraser, above n 96, at 95.

142 Hollis, above n 2, at 151–152.

143 At 153.

The development of an adequate legal response to the challenges of attribution would foster commitment to international law and respect for the rule of law. Such a response must be able to hold offending states responsible for their conduct despite the anonymity and uncertainty of cyber operations, and allow target states to have recourse to international law, in appropriate circumstances, when non-state actors carry out cyber operations which cause harm.[144] State practice following 9/11 has already moved towards self-defence against non-state actors. However, the emergence of a theoretical rule which addresses the major problems of attribution is still to be seen.

One compelling option is to adopt a due diligence standard of attribution in the cyber context. The due diligence standard of attribution is based on the general principle of due diligence, which imposes an obligation upon every state not to knowingly allow acts contrary to the rights of other states to be carried out from its territory.[145] But it departs from the dominant view of the due diligence principle as a primary rule of international law – the view adopted by the second International Group of Experts, who produced the *Tallinn Manual 2.0* as a restatement of the *lex lata*.[146] The due diligence standard of attribution works as a secondary rule of international law, attributing a cyber operation to a state when the state has knowledge that the cyber operation is being carried out from its territory contrary to the rights of another state, and nevertheless fails to take reasonable measures to prevent it. This makes the offending state directly responsible for the cyber operation.

Adopting a due diligence standard of attribution has the advantage of preserving the traditional conception of the right of self-defence, as applicable only in cases of armed attack by one state against another state. Thus, it avoids the question of why a host state should suffer an infringement of its sovereignty when self-defence is exercised directly against a non-state actor.[147] The due diligence standard of attribution appropriately limits potential state responsibility by narrowly defining the circumstances in which the standard will be breached: when a state has the requisite knowledge, whether actual or constructive, and fails to take reasonable measures.[148] So while the due diligence standard of attribution expands state responsibility beyond the scope of the Articles on State Responsibility, it is tempered by a clearly defined set of criteria.[149]

---

144 Chircop, above n 34, at 647.

145 *Tallinn Manual 2.0*, above n 3, at 30.

146 At 32.

147 Chircop, above n 34, at 664.

148 At 650.

149 At 651.

3 *Completeness*

If applying the *jus ad bellum* in the cyber context results in inaccurate and ineffective law, then the law is an incomplete regulatory response.[150] This is illustrated by the fact that no state has relied on the right of self-defence to respond to a cyber operation, nor has a state sought reparation for harm caused by a cyber operation from another state.[151] As seen in the Estonian and Georgian examples, the challenges of attribution in the cyber context prevents states from having recourse to the *jus ad bellum.* Therefore, in the absence of operative rules for state responsibility and other issues discussed in this article, cyberspace may effectively be a legal loophole.[152]

A complete regulatory response would require tailor-made rules for cyberspace, which may supplement or supplant rules applied by analogy.[153] New rules may emerge through state practice and *opinio juris*, or through agreement between states.[154] Many members of the original International Group of Experts believed that new rules were more likely to evolve through state practice and *opinio juris* than a formal, multilateral instrument such as a treaty.[155] This view is shared by other scholars.[156]

However, customary international law on the use of force changes slowly, unless an unprecedented event like 9/11 occurs, while IT evolves rapidly.[157] Furthermore, incremental legal development of new rules through state practice and *opinio juris* is particularly difficult in the cyber context due to the lack of transparency.[158] Recognising this problem, recently the United States of America, the United Kingdom and the Netherlands appear to be developing a name and shame culture in an attempt to increase regulation in cyberspace and counter alleged Russian cyber operations.[159] This may be one of the first steps towards a more accurate, effective and complete law for cyberspace.

---

150 Hollis, above n 2, at 153.

151 Chircop, above n 34, at 653.

152 At 653.

153 Hollis, above n 2, at 153–154.

154 At 153.

155 Schmitt, above n 57, at 1111.

156 For example, see Waxman, above n 58, at 153.

157 Fraser, above n 96, at 109–110.

158 Waxman, above n 58, at 154.

159 Fraser, above n 96, at 113; and "Transparency – the tool to counter Russia" (4 October 2018) BBC News <www.bbc.com/news>.

IV CONCLUSION

Cyberspace has captured much attention in the media and public discourse, as cyber operations play an increasingly extensive role in society. Take Estonia as an example. In 2016, 82 per cent of Estonians had internet access, and the state had moved much of its interactions with individuals online.[160] The 2007 cyber operations suffered by Estonia were the first instance of large-scale denial of service operations and were commonly described as "cyberwar" in the media.[161] Legally speaking, this description was inaccurate, but it appears that cyberspace has emerged as war's fifth domain.[162] As such, it needs to be appropriately regulated to maintain international peace and security.

Thus far, state practice and legal scholarship have generally concluded that the *jus ad bellum* applies to cyber operations. The normative rationale for this is that it offers a degree of certainty and constraint on state behaviour in what would otherwise be a legal loophole. The *jus ad bellum* provides that the use of cyber force is prohibited unless authorised under Chapter VII of the UN Charter or exercised in self-defence. However, the existing principles of international law do not necessarily translate well to cyberspace. This article has identified the areas in which the *jus ad bellum* does not work well and the gaps in which tailor-made rules for cyberspace are most needed.

Applying the existing international law principles by analogy to conventional warfare, the definition of a cyber use of force usually requires physical effects. A cyber armed attack likely always requires physical effects. This fails to recognise that cyber operations with non-physical effects may cause harm which threatens the welfare of a state critically dependent upon its information systems. Furthermore, the law of state responsibility does not mesh well with the anonymity of cyber operations, making the *jus ad bellum* difficult to enforce. As such, the definition of cyber use of force and cyber armed attack, and the problems of attribution, are the most pertinent issues hindering the accuracy, effectiveness and completeness of the *jus ad bellum* in the cyber context.

To address these issues, this article recommends two changes to the *jus ad bellum* in the cyber context. The first is to adopt an informational approach to the harm caused by cyber operations, to account for both physical and non-physical effects when determining whether there has been a cyber use of force. The second is to adopt a due diligence standard of attribution, which involves applying the general due diligence principle as a secondary rule of international law, to effectively hold offending states responsible for their conduct and allow target states to have recourse to international law in response to the conduct of non-state actors. If the most pertinent issues of defining cyber use of force and cyber armed attack, and attributing cyber operations are resolved, then the existing principles of international law may provide a useful foundation upon which to build the law on the

160 Haataja, above n 69, at 182–183.

161 At 160.

162 Fraser, above n 96, at 87.

use of force in cyberspace. New rules are likely to develop through state practice and *opinio juris* rather than through a formal, multilateral instrument. But the development of new rules through state practice and *opinio juris* depends upon greater transparency from states about how they respond to cyber operations.