FROM DATA TO DESTRUCTION: THE LEGAL CHALLENGES OF BIG DATA ATTACKS[*]

Veriden Yıkıma: Büyük Veri Saldırılarının Hukuki Zorlukları

Berkant AKKUŞ[**]

L&JR
Year: 16, Issue: 30
July 2025
pp.75-108

Article Information

Submitted : *19.01.2025*
Revision Requested : *07.03.2025*
Last Version Received : *27.03.2025*
Accepted : *22.04.2025*

Article Type

Research Article

ABSTRACT

The rapid development of technology has produced hugely positive outcomes, yet such benefits are placed in the shadow of the threat of the inappropriate use of technology. Incidents involving cyber-attacks have posed challenges to traditional international law on armed force and the right to self-defence. This study critically evaluates this issue, with focus on how the existing legal framework applies to cyber operations, and the challenges and issues that this gives rise to. The study explores the conditions under which cyber operations amount to a use of force giving rise to the right to use force in self-defence. With reference to big data attacks, the study argues that while the notion of implementing a new international legal instrument may appear to be a promising solution, it promises to create more problems than it remedies. Accordingly, big data attacks that exist beyond the armed force context cannot be reasonably deemed to reach the threshold of armed force. Furthermore, the extension of the existing legal framework to cyber operations, although it is not without challenges, has thus far proven more beneficial than problematic. It is predicted that existing issues will be gradually resolved as practical situations arise.

Keywords: Cyber operations, big data attacks, use of force, international law.

[*] There is no requirement of Ethics Committee Approval for this study.

[**] Asst. Prof., Inonu University, Faculty of Law, Department of Public International Law, Malatya/Türkiye, E-mail: berkantakkus91@gmail.com, ORCID ID: 0000-0001-6652-2512.

ÖZET

Teknolojinin hızlı gelişimi büyük olumlu sonuçlar doğurmuş olsa da, bu tür faydalar teknolojinin uygunsuz kullanım tehdidiyle gölgelenmektedir. Siber saldırılarla ilgili olaylar, silahlı kuvvet ve meşru müdafaa hakkı konusundaki geleneksel uluslararası hukuka meydan okumaktadır. Bu çalışma, mevcut yasal çerçevenin siber operasyonlara nasıl uygulandığını ve bu durumun ortaya çıkardığı zorluklar ile sorunları ele alarak bu konuyu eleştirel bir şekilde değerlendirmektedir. Çalışma, siber operasyonların hangi koşullar altında kuvvet kullanımı olarak değerlendirilebileceğini ve meşru müdafaa hakkını doğurduğunu araştırmaktadır. Büyük veri saldırılarına atıfta bulunarak, yeni bir uluslararası hukuk aracı uygulama fikrinin çekici bir çözüm gibi görünse de, aslında düzelttiğinden daha fazla sorun yaratacağını savunmaktadır. Buna göre, silahlı kuvvet bağlamının ötesinde var olan büyük veri saldırıları, makul bir şekilde silahlı kuvvet eşiğine ulaştığı düşünülemez. Ayrıca, mevcut yasal çerçevenin siber operasyonlara genişletilmesi, zorluklar barındırsa da, şu ana kadar sorunlardan çok fayda sağlamıştır. Mevcut sorunların, pratik durumlar ortaya çıktıkça kademeli olarak çözüleceği öngörülmektedir.

Anahtar Kelimeler: Siber operasyonlar, büyük veri saldırıları, kuvvet kullanımı, uluslararası hukuk.

INTRODUCTION

Cyber-attacks are cyber operations that are aimed at the alteration, deletion, corruption or denial of access to computer software or data, with the purposes of deception or propaganda, the partial or total disruption of the functioning of the target computer, or computer network or system, and related infrastructure, and physical damage which is extrinsic to the targeted computer, computer network or system.[1] A key characteristic of cyber operations is that they spread with great speed. For example, a computer worm attacked the database software of Microsoft in 2003, which spread throughout the entire internet over just 48 hours.[2] The worm caused significant harm by cancelling airline flights, causing failures in ATMs, interfering with elections, and network outages.[3] A further example is the distribution of a denial-of-service attack in Estonia in 2007, which brought governmental services and the banking system to a halt.[4] In 2010, a power plant in Iran was the target of a cyber-attack, which caused the

1 Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 17.

2 Heather Dinniss, *Cyber Warfare and the Laws of War* (CUP 2012) 296.

3 Eric Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-defence' (2002) 38 *Stan. J. Int'l L.* 207, 209.

4 Dinniss (n 3) 38.

rotor speed of its centrifuges to change, resulting in severe damage.[5] These are some of many examples of the speed and extent of the damage and disruption that cyber operations can cause.

As technology continues to develop at a rapid pace, the threat of cyber operations has become all the more apparent. This serves to demonstrate the significance of the study; in that it addresses a contemporary and pressing issue. Accordingly, the study examines the implications of cyber operations for international law. The key research question is: what implications do cyber operations have for the existing legal framework on the use of force? This gives rise to a range of research objectives. The first is to identify the key elements of international law on the use of force, and how they apply to cyber operations. The second is to examine whether cyber operations qualify as a use of force, and the implications of this for big data attacks. The third is to assess the various legal criteria on the use of force, and whether they apply effectively to cyber operations, or whether problems and gaps exist. The fourth is to explore the criteria for self-defence against cyber operations, with particular focus on whether, and under which circumstances, cyber operations and big data attacks amount to an armed attack under international law. The final objective is to critically explore whether existing problems and gaps would be best remedied by clarifying the scope and content of the existing legal framework, or developing a new, distinct, international legal instrument on cyber operations.

The research features doctrinal legal analysis. It is recognised that analysis of a legal issue cannot be effectively or accurately undertaken without first identifying the relevant and applicable legal framework.[6] Doctrinal legal analysis is the logical starting-point for the topic, given its legal character, and that it seeks to "describe a body of law and how it applies" to the specific context.[7] Doctrinal legal analysis therefore involves examination of key treaties, such as the Charter of the United Nations 1945 (UN Charter), case law, and legal commentary on cyber operations and the use of force. Some case studies are also used, to provide a practical dimension to the study. This involves analysis of recent data-centric cyber incidents, to assess their impact on state security, and to demonstrate the important limits that are placed on the scope of the use of force under international law. Finally, policy analysis is applied to evaluate international policies that address whether cyber operations amount to armed attacks giving rise to the right to use self-defence.

---

5 Roscini (n 2) 53.

6 MD Pradeep, 'Legal Research-Descriptive Analysis on Doctrinal Methodology' (2019) 4 *International Journal of Management, Technology and Social Sciences* 95, 97.

7 Ian Dobinson & Francis Johns, 'Legal Research as Qualitative Research' in *Research Methods for Law* (Mike McConville & Wing Hong Chui eds, 2nd edn, Edinburgh University Press 2017) 21.

The definition of big data varies depending on the context, and international law has yet to establish a universally accepted definition. One way to understand big data is through its sheer volume. As the term big implies, its defining characteristic is the vast amount of information it encompasses. One definition describes big data as "the exponentially increasing amount of digital information being generated by emerging technologies such as mobile internet, cloud storage, social networking, and the Internet of Things, along with the advanced analytics used to process it."[8] In essence, the technological ecosystem developed over the past decade has become the most extensive data mining operation in human history.

However, volume alone does not fully define big data. Another approach emphasizes its networked nature. The significance of big data lies not only in its size but in its ability to reveal patterns, establish connections between individuals, and generate insights. Its analytical capacity transforms it from a mere collection of vast datasets into both an opportunity and a challenge.

When combined with machine learning and algorithmic tools, big data enhances our ability to analyze and interpret complex information. Scholars note that "algorithms are used to analyze these large and unconventional data streams to uncover increasingly granular correlations between data points."[9] However, this analytical power has also been criticized for its potential to produce inaccurate, biased, and discriminatory outcomes.

What are the implications of big data for *jus ad bellum*? First, this legal framework can no longer treat data as a singular entity. Some data is discrete and individualized, while other data exists on a much larger scale. Big data stands apart due to both its volume and its analytical nature. Over time, states will likely establish clearer distinctions between cyber operations targeting big data—where the scale and effects may meet the threshold for the use of force—and those that do not. Second, legal scholarship on cyber operations must account for the differences in volume, impact, nature, and sensitivity between small data and big data. These distinctions will play a crucial role in shaping future legal interpretations.

The study commences with an outline of the key elements of the use of force under international law, namely, Article 2(4) of the UN Charter. This section proceeds to examine whether cyber operations qualify as a use of force. With reference to the Tallinn Manual, the various elements of the use of force are examined, such as state attribution, the use of force, and the threat of force. Section 3 examines the applicable law on self-defence and responses to cyber

---

8 Paul Symon & Arzan Tarapore, 'Defense Intelligence Analysis in the Age of Big Data' (2015) 79 *Joint Force Quarterly* 5.

9 Caryn Devins, Teppo Felin, Stuart Kauffman, Roger Koppl, 'The Law and Big Data' (2017) 27 *Cornell Journal of Law and Public Policy* 357, 363.

operations, with reference to big data attacks, with identification of strengths and weaknesses in the framework's application to cyber operations. Focus is placed on the principles of state attribution in the context of self-defence, whether cyber operations may amount to armed attacks, and how the principles of necessity and proportionality apply. Section 4 offers and explores recommendations for improvement, with focus on the implementation of a new legal framework that specifically addresses cyber operations, and the alternative of clarifying the extended application of the existing framework. The study ultimately draws a number of conclusions. The first is that there are challenges in the application of the existing international framework to cyber operations, but these can be resolved through practice, and as situations arise. The second is that classifying big data attacks as a use of force is not appropriate, and risks distorting the very spirit of the law on the use of force. Finally, the study argues that the most appropriate solution is to continue evolving the existing legal framework so that it more effectively encompasses cyber operations. The enactment of a new legal instrument would prove more problematic than beneficial.

I. CYBER OPERATIONS AND THE USE OF FORCE

A. The Scope of the Use of Force

Article 2(4) of the UN Charter provides that Member States:

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

There is no official or formal definition of 'threat or use of force'.[10] This is in recognition of the need for flexibility, and the various contexts to which the term may be applied. However, it is possible to observe that 'force', when considered in light of the purpose and spirit of the UN Charter, is limited to 'armed force'.[11]

The use of the term 'armed' implies that the force must involve the use of some form of a weapon, which is intended to kill or injure. It has been argued that almost any object can be utilised as a weapon, provided the intention is hostile.[12] The flexibility of Article 2(4) of the UN Charter is demonstrated in the *Nuclear Weapons Case,*[13] in which the International Court of Justice (ICJ) ruled

---

10 Marco Roscini, 'Threats of Armed Force and Contemporary International Law' (2007) 54 *Netherlands International Law Review* 229, 231.

11 Katharina Ziolkowski, *Stuxnet: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence 2012) 8.

12 John Yoo, 'Using force' (2004) 71 *University of Chicago Law Review* 729, 739.

13 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, para.

that Articles 2(4) and 51 (on the use of force in self-defence) of the UN Charter "do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed".[14] For example, the use of chemical and biological weapons does qualify as a use of force, implying that cyber operations should also qualify as such.[15] This is supported by the *Nicaragua Case,*[16] in which the ICJ categorised the training and arming of contras as a threat or use of force, implicitly recognising that the use of non-kinetic force may amount to a violation of Article 2(4) of the UN Charter.[17]

B. Do Cyber Operations Qualify as a Use of Force?

According to Rule 68 of the Tallinn Manual (Manual):[18]

> *"a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any state, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful".*

This rule reflects both Article 2(4) of the UN Charter and customary international law. In order for Article 2(4) of the UN Charter to apply to cyber operations, three conditions must be fulfilled. Firstly, the cyber operation must be attributed to a state, which excludes the conduct of armed groups or private individuals, irrespective of the damage caused.[19] Secondly, the cyber operation must amount to a threat or use of force.[20] Finally, the threat or use of force must be exercised in the context of international relations.[21]

Big data attacks refer to cyber operations that manipulate, steal, or destroy massive datasets, often targeting sensitive information, including financial data, military intelligence, and humanitarian records. On the one hand Tallinn Manual

39. (hereafter *Nuclear weapons Case*).

14 Ibid., para. 39.

15 Andrew Bell, 'Using Force against the Weapons of the Weak: Examining a Chemical-Biological Weapons Usage Criterion for Unilateral Humanitarian Intervention under the Responsibility to Protect' (2013) 22 *Cardozo J. Int'l & Comp. L.* 261, 266.

16 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)* (1986) ICJ Rep 14, para. 228 (hereafter *Nicaragua Case*).

17 Ibid., para. 228.

18 Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) (hereafter, *Manual*).

19 Garrett Derian-Toth and others, 'Opportunities for Public and Private Attribution of Cyber Operations' (2021) 12 *Tallinn Paper Series* 8, 9.

20 Herbert Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 *J. Nat'l Sec. L. & Pol'y* 63, 66.

21 Roscini (n 2) 44-45.

1.0: limited discussion on data. First, Tallinn Manual 1.0 primarily focused on cyberattacks causing physical or infrastructure damage. Second, Tallinn Manual 1.0 did not consider data as an independent target under IHL. Third, Tallinn Manual 1.0 did not address cyber threats to humanitarian or biometric data. On the other hand Tallinn Manual 2.0: recognizing data as a legal concern. For instance, data as a civilian object (Rule 100): Debate emerged over whether data, like physical infrastructure, should be protected under IHL. While Tallinn Manual 2.0 does not explicitly classify data as a protected civilian object, some experts argue that targeting vital data could violate the principle of distinction. Further, misinformation & fake news (Rule 113): The use of cyber operations to manipulate public perception or influence political stability through data-driven disinformation campaigns was addressed. In addition, humanitarian data protection: Cyberattacks targeting refugee databases or medical records pose ethical and legal dilemmas under IHL.

The Tallinn Manual 2.0 represents a significant expansion beyond the original 2013 edition, moving from a narrow focus on cyber warfare to a broader framework encompassing peacetime cyber activities and data-driven threats. While Tallinn Manual 1.0 only addressed cyber warfare, Tallinn Manual 2.0 incorporates state sovereignty, due diligence, and economic cyberattacks, making it more applicable to modern threats. The growing recognition of data as a strategic target introduces new challenges for international law, especially in humanitarian contexts but still there are unresolved questions for future legal developments. For instance, should data be classified as a civilian object under IHL? Can cyberattacks causing purely economic damage justify self-defense under Article 51 of the UN Charter? How should international law regulate misinformation campaigns in armed conflicts?

C. State Attribution

According to Rule 10 of the Manual, the prohibition of the threat or use of force is binding on all UN Member States, and is not binding on non-state actors, unless their acts can be attributed to a state, under the law of state responsibility. In the context of state attribution, the problems surrounding the identification of the attribution and origin of cyber operations to states are problematic, and pose a prominent hindrance to the application of Article 2(4) of the UN Charter to cyber operations. It is recognised that non-state actors are both willing and able to use force against states, and therefore, the prohibition of the threat or use of force should encompass non-state actors that are not attributable to a state.[22] The ICJ has demonstrated its willingness to include indirect uses of force

[22] Ankit Lavania, 'The Need to Fill Legal Vacuum in International Law to Deal with Non-State Actors in Cyber Operations' (2022) 5 *Int'l JL Mgmt. & Human.* 462, 465.

within the scope of Article 2(4) of the UN Charter.[23] There is an opportunity for the attribution criteria to be interpreted in a more extensive manner to include the activities of non-state actors, although there remain some circumstances in which non-state actors act independently to states.

Non-state actors – at the very least those who demonstrate some degree of organisation – should be perceived as bound by the international customary law that prohibits the threat or use of force. The customary international rule should therefore be applicable to non-state actors, because their acts that amount to a threat or use of force impact the fundamental right that underlies Article 2(4) of the UN Charter and customary international law.[24] This is the right to remain free from the threat or use of force.[25] To permit non-state actors to violate this right would undermine the very purpose and spirit of the prohibition of the threat or use of force.

In the context of international organisations, the Manual clarifies that:

> *"International organisations bear international legal responsibility for their cyber activities and cyber-related omissions that constitute internationally wrongful acts".*[26]

Due to their status as subjects of international law, international organisations are bound by customary international law.[27] However, the Manual itself recognises that "the binding nature of many customary norms *vis-à-vis* international organisations is unsettled".[28] The result is that international organisations are subject to customary primary norms in non-cyber contexts and "fully in the cyber context".[29]

D. The Use of Force

Rule 69 of the Tallinn Manual states that "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".[30] The definition of 'force' is crucial in this respect,

---

23 *Nicaragua Case,* para. 228.

24 Michael Schmitt and Sean Watts, 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace' (2016) 21 *Journal of Conflict and Security Law* 595, 606.

25 Nicholas Tsagourias, 'Non-State Actors and the Use of Force' in *Participants in the International Legal System: Theoretical Perspectives* (Jean D'Aspremont ed, Routledge 2011) 327-328.

26 Manual, Rule 4.1.

27 Manual, Rule 4.5.

28 Ibid.

29 Ibid.

30 See: *Nicaragua Case,* para. 195.

in that it implies that big data attacks do not lie within its scope.[31] The Manual adopts an effects-based rather than an instrument-based approach, reflecting the widely held view that the use of force should be separate from the instrument used.[32] Therefore, Rule 69 of the Manual confirms that any force that has harmful effects in the form of human injury/death and/or physical damage equivalent to those resulting from military force are in violation of the prohibition, which includes cyber force (and excludes big data attacks). However, there remains the question concerning whether cyber operations that are committed against the critical infrastructure of a state, which do not cause physical harm, but which have the effect of severely disrupting state functioning amount to a use of force under Article 2(4) of the UN Charter. This would potentially include big data attacks. Rule 69.2 implies that political or economic coercion is to be excluded from the definition of force, based on the *travaux preparatoires* of the UN Charter, and the UN General Assembly's Declaration on Friendly Relations 1970. However, this does not mean that cyber operations that have a serious impact on critical infrastructure do not qualify as a use of force. This is apparent in Rule 69.10, in which it is recognised that: "some may categorise massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful". This further demonstrates the effects-based approach adopted by the Manual, and suggests that big data attacks will rarely meet the necessary threshold. Therefore, data breaches that primarily cause economic damage will be highly unlikely to fall within the scope of Article 2(4) of the UN Charter.[33] It is argued that this is an appropriate approach, given the implications of the qualification of a cyber operation as a use of force. When such attacks result in the injury or death of persons, and/or the destruction of property, only then is it acceptable to define them as a use of force, lest the scope and meaning of the use of force become distorted.

Upon closer analysis, the Manual does not explicitly exclude cyber operations that damage critical infrastructures from the definition of force. The Manual clarifies that "generating mere inconvenience or irritation will never" amount to a use of force.[34] However, it proceeds to discuss the factors that may be taken into account when determining whether cyber operations are an unlawful use of force. In outlining the concept of severity (the central factor), the Manual states that "the more consequences impinge on critical national interests, the more

---

31 Terence Check, 'The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure' (2022) 13 *Nat'l Sec. L. Brief* 1, 4.

32 Consistent with *Nuclear Weapons Case*, para. 39.

33 Lianne Boer, 'Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace' (2013) 5 *Amsterdam LR* 4, 6.

34 Manual, Rule 69.9a.

they will contribute to the depiction of a cyber operation as a use of force".[35] At this point, "the scope, duration, and intensity of the consequences" are of vital significance in determining severity.[36] Thus the severity criterion measures the range of consequences of an attack, including but not limited to physical consequences. Therefore, cyber operations that have severe consequences for critical infrastructure may qualify as a use of force, regardless of whether physical damage was caused.[37] However, it is unlikely that this will include the effects of big data attacks, because they do not meet the necessary threshold. Big data attacks—such as the manipulation, destruction, or exploitation of vast datasets—could, in some cases, meet the necessary severity threshold. However, the applicability depends on the effects-based approach widely used in cyber law assessments. Some considerations include: If a big data attack directly results in kinetic effects—such as manipulating health data in a way that causes physical harm or misdirecting military operations—it could cross the use of force threshold. For example, altering medical records in a conflict zone to prevent necessary treatments could have life-threatening consequences. While economic coercion alone typically does not qualify as a use of force (as seen in ICJ jurisprudence), a big data attack that causes widespread systemic failures—such as in financial systems, food distribution, or critical infrastructure—could push the threshold if the disruption leads to significant harm. If an adversary manipulates or degrades military AI decision-making systems using big data attacks, causing battlefield miscalculations or increased casualties, the severity threshold may be met. For a cumulative approach where a series of cyber operations, including big data manipulations, collectively result in harm comparable to traditional kinetic attacks. If a pattern of such attacks leads to widespread suffering or military disadvantage, it may be considered a use of force.

The Manual imposes further limits of the scope of the use of force, by imposing a *de minimis* scale and effects threshold, which establishes a distinction between acts that do and do not qualify as a use of force under Article 2(4) of the UN Charter.[38] Rule 69.6 of the Manual refers to the ICJ's distinction drawn between the grave and less grave forms of the use of force in the *Nicaragua Case*.[39] In applying this judgement, the Manual confirms that the most grave uses of force will constitute an armed attack, giving rise to the right of self-defence, whereas less grave uses of force will constitute a violation of Article 2(4) of the

35 Manual, Rule 69.9a.

36 Ibid.

37 Terence Check, 'The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure' (2022) 13 *Nat'l Sec. L. Brief* 1, 4.

38 Divij Kumar, 'Interpretation of International Law under the Tallinn Manual(s)' (2021) 3 *Indian JL & Legal Rsch.* 1, 3.

39 *Nicaragua Case,* para. 191.

UN Charter.[40] However, the Manual does not clarify the criteria applicable for measuring the gravity of a use of force, implying the aim to achieve flexibility, and to provide a broad margin of appreciation in this respect.[41] The Manual does identify this issue, and stipulates that states may take a range of factors into account when determining whether or not a cyber-attack amounts to a use of force: Severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive illegality.[42] These factors do not have legal status and are not exhaustive,[43] and whether they offer meaningful guidance is subject to debate.

Arguably, more precise thresholds are required in order to effectively guide states in determining whether cyber operations amount to a use of force. For example, cyber operations may feature a considerable length of time between the insertion of a particular vulnerability into a target system, its execution, and the damage caused.[44] Furthermore, cyber operations (as well as big data attacks) involve a range of stages, each of which directly and indirectly contribute to the outcome, and which introduces uncertainty in the context of the principle of directness. The directness and immediacy principles are particularly problematic, because a cyber operation's most severe consequences may be non-immediate and indirect.[45] This fails to recognise that cyber operations and big data attacks have both immediate and long-term, and direct and indirect effects. The measurability of effects principle is also potentially problematic, because it is often difficult to measure overall harm inflicted on a state, particularly when the majority of the consequences are indirect, or involve big data.[46] The problem with the principle of state involvement is that there are often major difficulties involved in attributing cyber operations to states, due to their anonymity and multi-staged nature.[47] Finally, distinguishing between lawful and unlawful cyber operations is by no means straightforward. For instance, inserting a vulnerability may be

---

40 Manual, Rule 69.6.

41 Nicholas Tsagourias, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' (2012) 15 *Yearbook of International Humanitarian Law* 19, 32.

42 Manual, Rule 69.9a-d.

43 Manual, Rule 69.7.

44 Andrew Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate' (2012) 67 *Joint Force Quarterly* 40, 44.

45 Tsagourias (n 42) 28.

46 Shannel Gunatileka, '"Big Data Breaches", Sovereignty of States and the Challenges in Attribution' (2024) 5 *University of Colombo Review* 104, 119.

47 David Clark & Susan Landau, 'Untangling Attribution' in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (National Research Council 2010) 25.

unlawful, yet it may also amount to some other act that is not prohibited under international law.[48]

The introduction of a *de minimis* threshold achieves little in terms of promoting certainty and clarity. This may lead to assessments as to whether cyber operations and big data attacks amount to a use of force being challenged. However, cyber operations that do not fall within the scope of Article 2(4) of the UN Charter will not automatically be deemed legal. As the Manual states, they may qualify as an unlawful intervention;[49] a concept which is considerably broad.[50] The element of coercion is the key element that distinguishes between interference and intervention.[51] Intervention is coercive in that it causes a state to do something that it would not do otherwise. The principle of intervention therefore provides a secondary net, enabling acts that do not qualify as a use of force to amount to unlawful intervention.

E. A Threat of Force

Rule 70 of the Manual provides that an actual or threatened cyber operation amounts to an unlawful threat of force "when the threatened action, if carried out, would be an unlawful use of force". This mirrors the definition of unlawful threat of force set out by the ICJ in the *Nuclear Weapons Case.*[52] Therefore, all threats of force except the threat of the use of force by self-defence or under Chapter VII of the UN Charter are not lawful.[53] In order for an unlawful threat of force to be found, it is not necessary that the threat be accompanied by a specific or particular demand. However, coercion lies at the very epithet of a prohibited threat of force.[54] A threat of force does pressure the target state irrespective of whether it includes a specific demand and a threat can be communicated in implicit or explicit form, though conduct or words.[55] Whether such communication amounts to a threat of force is highly context-specific, and depends on a range of factors. What is clear is that "actions that simply endanger the security of the target state, but that are not communicative in nature, do not qualify" as a threat of force, suggesting that big data attacks do not meet the threshold.[56]

---

48 Dan Efrony & Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 *American Journal of International Law* 583, 611.

49 Manual, Rule 69.6-10.

50 *Nicaragua Case*, para. 246.

51 Ibid, para. 205.

52 *Nuclear Weapons Case*, para. 47.

53 Manual, Rule 70.3.

54 Manual, Rule 70.4.

55 Ibid.

56 Manual, Rule 70.4.

This clarifies that there must be a communicative element. While this appears logical, such an approach is rather restrictive, because it fails to take context into account, such as political, historical and military factors. Taking such factors into account may lead to the inference that a threat of force has been made by the mere development or acquisition of cyber capabilities. The approach adopted by the Manual fails to recognise the subjectivity of assessments as to whether a threat of force exists.[57]

II. DEFENCES OR RESPONSES TO CYBER ATTACKS

Big data attacks, when they only result in economic damage, do not, and should not reach the threshold of the use of force. Accordingly, states should not be permitted to exercise force in self-defence against such attacks. However, if economic damage is accompanied by injury or death, or destruction of property, the right of self-defence may be exercised, provided the requirements are met. These requirements are examined in this section.

It is important to point out that some have argued in favour of equating big data attacks to the use of force under international law.[58] Such arguments are based on the interpretation of big data as a resource, which is a potential target during armed conflict. However, the law is clear, that economic damage, at least that inflicted by big data attacks, does not meet the requisite threshold. This is not without reason; the use of force must be kept within certain boundaries, given the implications of equating a cyber operation with a use of force. Furthermore, the Manual clarifies that data is an intangible asset, and therefore not an object, meaning that it does not fall within the scope of the 'destruction of property' element.[59]

A. The Use of Force in Self-Defence

As has been clarified, international law generally prohibits the use of force. However, a vital exception to this general prohibition is the use of force in self-defence.[60] Article 51 of the UN Charter provides for the right to use force in self-defence, presenting it as the "inherent right of individual or collective self-defence if an armed attack occurs". Rule 71 of the Manual provides for the right to self-defence against armed attack, stating that "a state that is the target of a cyber operation that rises to the level of an armed attack may exercise its

---

57 Duncan Hollis and Tsvetelina Van Benthem, *Threatening Force in Cyberspace* (Temple University Legal Studies Research Paper 2021) 13.

58 Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 *NYUJ Int'l L. & Pol.* 57, 60.

59 Tallinn Manual, Rule 100.6.

60 Gleider Hernandez, *International Law* (OUP 2019) 352.

inherent right of self-defence". This reflects the ICJ's approach towards self-defence, which is subject to the requirement that self-defence only be in response to a cyber operation equivalent to an armed attack.[61]

A cyber use of force amounts to an armed attack in the event that it has grave scale and effects.[62] However, the ICJ has not clarified how the gravity of an attack may be measured, which the Manual recognises but does not elucidate on.[63] This is problematic, because it gives rise to the potential for differing interpretations of any given cyber operation. This creates uncertainty surrounding whether a cyber operation may be deemed an armed attack for the purpose of self-defence.[64] This is apparent in the context of the SolarWinds hack, whereby hackers deployed a malicious code – a supply chain attack – into the monitoring and management software of SolarWinds Orion system 2020.[65] The hackers gained access to the systems, networks and data of thousands of customers and partners, which included state, local and federal agencies. It was believed that Russia's Foreign Intelligence Services was responsible for the hack, although the Russian government denied any involvement.[66] The incident highlights disagreement surrounding the appropriate standard for the qualification of cyber operations as a use of force, although it is widely accepted that it did not cross the threshold of the use of force,[67] because it did not result in any physical damage, death, injury, or destruction of property. This places a clear boundary, requiring that physical damage, death, injury, or destruction of property result from a big data attack in order for it to amount to a use of force. While there were significant economic costs, they were not at a level that might have justified the characterisation of the incident as a use of force. Arguably, this is appropriate, because it imposes significant boundaries on the scope of the concept of the use of force in the context of cyber operations.

A further question is whether attacks committed by non-state actors that are not attributable to a state qualify as an armed attack giving rise to the right

---

61 *Nicaragua Case*, para. 191; *Oil Platforms Case (Islamic Republic of Iran v United States of America)* (2003) ICJ Rep 4, para. 51 (Hereafter, *Oil Platforms Case*).

62 Manual, Rule 71.3-6.

63 *Nicaragua Case*, para. 195; Manual, Rule 71.7.

64 Kosmas Pipyros, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis & Theodoros Apostolopoulos, 'A New Strategy for Improving Cyber-Attacks Evaluation in the Context of Tallinn Manual' (2018) 74 *Computers & Security* 371, 377.

65 Massimo Marelli, 'The SolarWinds Hack: Lessons for International Humanitarian Organizations' (2022) 104 *International Review of the Red Cross* 1267, 1271.

66 Antonio Coco, Talita Dias & Tsvetelina Van Benthem, 'Illegal: The SolarWinds Hack under International Law' (2022) 33 *European Journal of International Law* 1275, 1278.

67 Kristen Eichensehr, 'Not Illegal: The SolarWinds Incident and International Law' (2022) 33 *European Journal of International Law* 1263, 1266.

of self-defence.[68] While the general view is that this does give rise to the right to self-defence,[69] there is disagreement surrounding this view. The ICJ has in several judgements determined that only a state can commit an armed attack.[70] However, dissenting judges have criticised this stance.[71] It is argued that the correct view is that non-state actors can commit an armed attack, according to international customary law on self-defence, and Article 52 of the UN Charter.[72] This view is further supported by the Security Council, which in Resolutions 1368 and 1373 (2001) determined that the Al Qaeda attacks amounted to an armed attack, giving rise to the right of self-defence.[73] However, there is evidence to the contrary. It has been argued that it is implicit in Article 51 of the UN Charter that a state rather than a non-state actor must commit an armed attack in order for the right to self-defence to be exercised.[74] This was confirmed in the *Palestinian Wall Case,*[75] in which the ICJ ruled that self-defence cannot be exercised against non-state actors. The International Criminal Court (ICC) has also confirmed that Article 51 of the UN Charter only offers the right of self-defence "in the case of an armed attack *by one state against another state*".[76] Armed attacks against non-state actors are considered a violation of the target state's territorial integrity and are permissible only when the non-state actor's actions can be attributed to the target state..[77] This is problematic, given the

---

68 Manual, Rule 71.

69 Carlo Focarelli, 'Self-Defence in Cyberspace' in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias & Russell Buchan eds, Edward Elgar Publishing 2021) 324; Noam Lubell, *Extraterritorial Use of Force Against Non-State Actors* (OUP 2010) 25-42.

70 Manual, Rule 71.15-17; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (2004) ICJ Rep 28, para. 139

71 *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (2004) ICJ Rep 28, para. 139, Contra: Judge Higgins Separate Opinion, paras. 33-34; Judge Kooijmans Separate Opinion, paras. 35-36 (Hereafter *Palestinian Wall Case*); *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v Rwanda*) (2006) ICJ 6, para. 146, Contra: Judge Kateka Dissenting Opinion, para. 34 (Hereafter, *Armed Activities Case*).

72 Also: *Caroline v United States,* 11 U.S. 496 (1813).

73 United Nations Security Council (UNSC) Res 1373 (28 September 2001) UN Doc S/RES/1373; United Nations Security Council (UNSC) Res 1368 (12 September 2001) UN Doc S/RES/1368.

74 Jutta Brunnee, 'The Security Council and Self-Defence: Which Way to Global Security?' in *The Security Council and the Use of Force* (Niels Blokker & Nico Schrijver eds, OUP 2005) 122.

75 *Palestinian Wall Case,* para. 35.

76 International Criminal Court, *Report of the Special Working Group on the Crime of Aggression*, ICC-ASP/7/ SWGCA/2 (2009).

77 Paola Reyes, 'Self-Defence against Non-State Actors: Possibility or Reality?' (2021) 9 *Revista Facultad de Jurisprudencia* 151, 154.

difficulties and challenges involved in attributing cyber-attacks to a state, which are explored in detail in the next section.

B. State Attribution and Self-Defence

The Manual explicitly confirms that the international customary law of state responsibility applies to cyber operations;[78] Rule 14 stipulates that states bear international responsibility for cyber-attacks that are attributable to them, and that constitute a breach of an international legal obligation. Rule 15 of the Manual outlines the principles of state attribution, which stipulates that all acts of force committed by state organs in an "official capacity",[79] under state authority,[80] organs "empowered by domestic law … to exercise elements of government authority",[81] and organs acting "under the exclusive direction and control" of the state.[82] In relation to the final category, disagreement surrounds whether the applicable threshold is effective control as was opined by the ICJ in the *Nicaragua Case* and the *Bosnia Genocide Case*,[83] or effective control in the context of organised groups, as the International Criminal Tribunal for the Former Yugoslavia opined in the *Tadic Case.*[84] The Manual rejects adopting a specific position on this issue, and simply defines 'effective control' as state control over the "execution and course of the specific operation and cyber-activity" which is integral to the operation.[85]

There are different criteria of attribution applicable to different situations and contexts, as the ICJ itself has stated.[86] Following the September 11 attacks, and prominently in the context of terrorist attacks, the criteria of unwillingness and toleration have also been identified,[87] which the ICJ was receptive to in the *Armed Activities* case.[88] Therefore, if a state tolerates and is unwilling to suppress groups that commit a cyberattack on another state, it will be attributable to that

78 Manual, Rule 4.4.

79 Manual, Rule 15.6.

80 Manual, Rule 15.7.

81 Manual, Rule 15.8.

82 Manual, Rule 16.2.

83 *Nicaragua Case*, paras. 116-117; *Bosnia and Herzegovina v Serbia and Montenegro* (2007) ICJ 2, paras. 402-406 (Hereafter, *Bosnian Genocide Case*).

84 *Prosecutor v Dusko Tadic* (1999) ICTY Appeals Chamber, IT-94-1-A, para. 131.

85 Manual, Rule 17.6.

86 *Bosnian Genocide Case*, paras. 404-405.

87 Bruno Simma, Daniel-Erasmus Khan, Georg Nolte & Andreas Paulus, *The Charter of the United Nations: A Commentary* (4th edn, OUP 2024) 1418.

88 *Armed Activities Case*, para. 147.

state, and be the target of self-defence operations.[89] The Manual does not address whether there are further criteria for attribution, or the extent to which a state that is unwilling to control non-state actors may amount to state complicity. This should depend on the extent to which the state involvement or complicity contributed to the possibility of the attack.[90] However, Rule 7 on due diligence clarifies that states are under the obligation to take all feasible measures to "put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other states". This implies that there are situations in which an attack may be attributed to a state when the state tolerates the launching of such attacks.

C. Are Cyber Operations Armed Attacks?

All armed attacks amount to a use of force, but not all uses of force amount to an armed attack that trigger the right to self-defence. As Article 51 of the UN Charter and customary international law provide, the act must be a grave use of force that causes severe injury and death and/or severe destruction and damage of property. This effects-based approach avoids the problems surrounding the definition of 'armed attack' that arise under the acts-based approach.[91] It focuses on the consequences of the action, rather than the weapons or means used, yet still has the effect of excluding most big data attacks from the scope of 'armed attack'.[92] Measured via the scale and effects approach, if such consequences are sufficiently severe to reach the threshold of an armed attack, the action will qualify as an armed attack, irrespective of the tools used to execute it. Thus, a conventional weapon need not be used to carry out an armed attack; attacks carried out by cyber means, provided they have sufficiently grave consequences to amount to an armed attack, also fall within this category. Cyber-attacks (and big data attacks) that cause substantial material destruction or harm may therefore qualify as armed attacks, triggering the right to self-defence.[93]

---

89 Yuki Motoyoshi, 'The Legal Framework of the 'Unwilling or Unable' Theory and the Right of Self-Defence against Non-State Actors' (2021) 37 *Nihon University Comparative Law* 25, 32.

90 Simma (n 88) 1416.

91 Paul Withers, 'Do We Need an Effects-Based Approach for Cyber Operations?' in *Research Handbook on Cyberwarfare* (Tim Stevens & Joe Devanny eds, Edward Elgar Publishing 2024) 214.

92 Michael Schmitt, 'Big Data: International Law Issues Below the Armed Conflict Threshold' in *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (Laura Dickinson & Edward Berg eds, Vol. 9, OUP 2024) 35.

93 Ido Kilovaty, 'Attacking Big Data as a Use of Force' *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (L Dickinson & E Berg eds, Vol. 9, OUP 2024) 144.

There are three distinct categories of the effects of cyber-attacks. First-order effects affect the specifically targeted system, while second-order effects are visible outside of the targeted system, although they are strictly linked to it, and third-order effects are long-term effects that result from the first- and second-order effects, and can be identified in political, strategic, and social changes within the target state.[94] However, this gives rise to the question concerning whether cyber-attacks and big data attacks that are directed against and severely disrupt national critical infrastructures, but do not cause damage to property or loss of human life, qualify as armed attacks which trigger the right to self-defence.[95] It has been argued that the severe disruption of national critical infrastructures caused by cyber-attacks, absent destruction of physical property or harm to persons, should amount to armed attacks.[96] This includes the severe disruption of industrial and economic infrastructures, which extends to big data attacks. However, this significantly extends the meaning of the term 'armed attack', enabling the right to self-defence to be exercised for a wider range of actions for which the term was not initially envisaged. Arguably, this is why the Manual does not include economic coercion within the scope of 'armed attack',[97] which excludes big data attacks that only cause economic damage. This once again appears to depend on the scale and effect principles, in that the Manual recognises that: "some may categorise massive cyber operations that cripple an economy as a use of force, even though economic coercion is presumptively lawful".[98] In the cyber context, the effects of a cyber operation that targets a state's economy would typically arise long after the completion of the operation. If this was to be deemed an armed attack, it would give rise to issues surrounding the immediacy and necessity of the target state's response. Therefore, it is generally the case that economic coercion falls outside of the scope of 'armed attack'.[99]

There are arguments in favour of including the severe disruption of national critical infrastructures within the scope of 'armed attack', which could also extend to big data attacks. Several states appear to defend this assertion; the US includes attacks that severely disrupt national critical infrastructures within

94 Venkata Palleti, Sridhar Adepu, Vishrut Mishra & Aditya Mathur, 'Cascading Effects of Cyber-Attacks on Interconnected Critical Infrastructure' (2021) 4 *Cybersecurity* 1, 8.

95 Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229, 238.

96 Avra Constantinou, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Sakkoulas 2000) 63-64.

97 Manual, Rule 69.2-3.

98 Manual, Rule 69.10.

99 Jacob Batinga, 'Reconciling the Global North-South Divide on the Use of Force: Economic Coercion and the Evolving Interpretation of Article 2(4)' (2024) 41 *Wis. Int'l LJ* 103, 106.

the scope of 'cyber attacks', giving rise to the right of self-defence.[100] If such a position was to be accepted, a cyber-attack directed against a state's financial system that causes severe economic instability should theoretically amount to an armed attack. However, to accept such a view would be to significantly extend the scope of the meaning of 'armed attack'. On the other hand, technological developments have enabled cyber-attacks to inflict serious harm on target states without specifically causing loss of human life or physical destruction – this is particularly the case with big data attacks. Even in the event that such circumstances were included within the scope of 'armed attack', this would not automatically give rise to the right to use force in self-defence against the perpetrator, given the need for necessity and proportionality. For example, measures that do not involve the use of force may be deemed viable alternatives, such as passive cyber defence, or cyber operations that do not reach the level of force.

The Manual recognises the lack of consensus on the issue of cyber-attacks that "do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects".[101] The Manual points out that such attacks are considered by some to amount to an armed attack, while others adopt the alternative view that they do not.[102] The former view places focus on the "extent of the ensuing effects" rather than the nature of the consequences.[103] Agreement has yet to be reached on this matter, rendering the question unanswered. This study argues that the effects-based approach adopted could potentially permit cyber-attacks (and big data attacks) that severely disrupt national critical infrastructures could amount to an armed attack, depending on the consequences. This would prove consistent with the overall approach adopted in the Manual, and allow for a context-specific approach to be adopted.

There is also debate surrounding whether a target state can use force in self-defence against a series of cyber-attacks that would not qualify as armed attacks alone, but may reach the necessary severity to qualify as an armed attack if considered collectively. Aggregated attacks that do not individually meet the threshold of an armed attack are not fully addressed in the Manual. It simply provides that such attacks will qualify as an armed attack if they are carried out by the same perpetrator, are related, and "taken together meet the requisite scales and effects".[104] The ICJ in the *Oil Platforms Case*[105] and the

100 Roscini (n 2) 74.

101 Manual, Rule 71.12.

102 Ibid.

103 Ibid.

104 Ibid., Rule 71.11.

105 *Oil Platforms Case*, para. 64.

Armed Activities Case[106] took into account the fact that there had been a series of attacks when determining whether an armed attack had taken place. However, it had not clarified this point of law, because it did not determine that there was an armed attack on alternative grounds. It has been opined by some scholars that attacks that are low in intensity could combine to amount to an armed attack for the purposes of self-defence.[107] However, this approach has been rejected by other scholars, and even Judge Simma in the *Oil Platforms Case.*[108] This issue therefore remains unclear, both for cyber operations and big data attacks. This study argues that considering a series of low intensity cyber-attacks collectively would enable them to reach the threshold to qualify as an armed attack. This is consistent with the effects-based approach, in that it would look to the cumulative effects of the cyber-attacks.[109] This would in fact resolve debate surrounding the inclusion of cyber operations that result in the severe disruption of national critical infrastructures, but which do not cause loss of life or material damage, within the scope of 'armed attack', giving rise to the right to self-defence. The scale and effects requirement would ensure that the cyber-attacks would need to have a sufficiently disruptive effect on national critical infrastructures to amount to an armed attack.[110]

D. Necessity, Immediacy and Proportionality

In the event that a state lawfully uses armed force under Article 51 of the UN charter, it is required to fulfil the requirements of necessity and proportionality. In order to satisfy the necessity requirement, the target state must use armed force in self-defence as a last resort to bring an end to the armed attack; non-forcible measures must not be available to end the armed attack.[111] The target state judges the principle of necessity - it is largely subjective in nature. In order to satisfy the proportionality requirement, the use of armed force in self-defence must be proportionate to the need to end the armed attack.[112]

A use of armed force in self-defence must also fulfil the imminence and immediacy requirements. This means that the armed attack must be imminent,

---

106 *Armed Activities Case*, paras. 146-147.

107 Yoram Dinstein, *War, Aggression and Self-Defence* (CUP 2010) para. 548; Carsten Stahn, 'Terrorist Acts as Armed Attack: The Right to Self-Defense, Article 51 (½) of the UN Charter, and International Terrorism' (2003) 27 *The Fletcher Forum of World Affairs* 35, 54.

108 *Oil Platforms Case,* Judge Simma, para. 14.

109 Tsagourias (n 96) 233.

110 Roscini (n 2) 75.

111 Suzanne Uniacke, 'The Condition of Last Resort' in *The Cambridge Handbook of the Just War* (L May ed, CUP 2018) 103.

112 David Kretzmer, 'The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum' (2013) 24 *European Journal of International Law* 235, 266.

and the response of the target state must immediately follow the occurrence of the armed attack.[113] These requirements are applied under Rule 72 of the Manual, which stipulates that "a use of force involving cyber operations undertaken by a state in the exercise of its right to self-defence must be necessary and proportionate". A target state can use active or passive cyber defence, and where passive defence measures are sufficient to prevent a cyber-attack, forceful active cyber defence measures are unlawful. Active cyber defence measures are attacks that respond to cyber-attacks that have already been carried out, and may be below or beyond the threshold of force. As the principle of necessity provides, if cyber defence operations are not sufficient to prevent a current or future armed attack, cyber armed force is permissible under the right of self-defence.[114] The principle of proportionality requires that the amount of force used in self-defence must be at the level required to prevent or cease an armed attack. A cyber use of force in response to a cyber-attack may not be sufficient, rendering a kinetic use of force permissible.[115]

The immediacy requirement stipulates that the self-defence must be aimed at preventing or stopping an armed attack, which excludes punishment for the armed attack. Thus, the self-defence response need not be instant in terms of the period of time following the armed attack.[116] Rather, it must be within a reasonable time following the armed attack. This principle is rather flexible, which is particularly appropriate in the context of cyber-attacks. This is because a considerable amount of time may be needed for a target state to identify a perpetrator. Furthermore, a cyber-attack may have debilitated the target state's ability to exercise self-defence. Thus, the immediacy requirement is able to take into account the particular aspects of cyber-attacks.

E. Anticipatory Self-Defence and Cyber Operations

The Manual permits a state to "act in participatory self-defence … when the attacker is clearly committed to launching an armed attack and the victim state will lose its opportunity to effectively defend itself unless it acts".[117] Although customary international law does contemplate the use of anticipatory countermeasures to deter an imminent armed attack, which includes cyber operations, international law does not provide for such countermeasures.[118]

---

113 Terry Gill, 'The Temporal Dimension of Self-Defence: Anticipation, Pre-Emption, Prevention and Immediacy' (2006) 11 *Journal of Conflict and Security Law* 361, 365.

114 Chris O'Meara, *Necessity and Proportionality and the Right of Self-defence in International Law* (OUP 2021) 58.

115 Roscini (n 2) 90.

116 James Green, 'The Ratione Temporis Elements of Self-Defence' (2015) 2 *Journal on the Use of Force and International Law* 97, 103.

117 Manual, Rule 73.4.

118 See: *Gabcikovo-Nagymaros Project* (*Hungary v Slovakia*) (1997) ICJ 692, para. 83.

The speed of cyber operations argues in favour of a permissive response to anticipatory countermeasures in such contexts.[119] Cyber operations feature a speed that is not present in many other systems of attack. However, they also require considerable time to develop, and become apparent in the systems of the target state. A target state may know of such actions, and have the ability to adopt countermeasures prior to the illegal attack, in order to decrease or eliminate its effectiveness. However, the target cannot lawfully do so, due to the fact that the countermeasures doctrine requires that an illegal act occur before action may be permitted.[120] A more effective approach would be to permit anticipatory countermeasures that are proportionate to the impending illegal act, and specifically focused on preventing it.

III. RECOMMENDATIONS FOR AN INTERNATIONAL LEGAL FRAMEWORK

While the Manual provides a useful basis for the regulation of cyber-attacks, it contains several gaps and weaknesses (as outlined in the previous sections), and lacks legally binding force. This gives rise to the question as to whether a binding international law framework should be established to regulate the specific context of cyber-attacks. Alternatively, the existing international law framework could be amended to explicitly provide for and clarify the legal position on cyber-attacks. This may prove problematic in the context of new situations, as Shaw recognises:

> *"one of the major problems of international law is to determine when and how to incorporate new standards of behaviour and new realities of life into the already existing framework, so that, on the one hand, the law remains relevant and, on the other hand, the system itself is not too vigorously disrupted".*[121]

In the context of big data attacks, the Manual is clear that such attacks do not amount to armed force, because data is not recognised as an object.[122] However, an increasing number of scholars and states have expressed that intangible data should be regarded as an object, subject to international law on the use of force.[123] For example, it has been suggested that damage caused to big data should relate

---

119 Gary Corn & Eric Jensen, 'The Use of Force and Cyber Countermeasures' (2018) 32 *Temp. Int'l & Comp. LJ* 127, 133.

120 Ryan Hayward, 'Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defence' (2017) 117 *Colum. L. Rev.* 399, 402.

121 Malcolm Shaw, *International Law* (7th edn, CUP 2014) 31.

122 Manual, Rule 102.

123 Michael Schmitt, 'The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision' (2015) 48 *Israel Law Review* 81, 85.

to the integrity, availability, and confidentiality of such data.[124] Some believe that cyber operations that cause economic injury *during an armed conflict* must comply with the principles of proportionality and necessity.[125] However, this relates to cyber operations *during* armed conflict, meaning that a big data attack does not automatically trigger the right to use force in self-defence outside of the armed conflict context. This demonstrates that international law primarily regulates big data attacks as part of armed conflict, and economic damage is not actionable outside of this context, which is a necessary limitation on the scope of the use of force in self-defence. To allow a big data attack that does not have immediate physical consequences to trigger an armed conflict cannot be reconciled with the foundations of the law on armed conflict. Alternatively, and firstly, it is necessary to determine whether cyber operations in general should be contained in a separate international legal instrument.

While treaties are legally binding, they are only binding on the states that are parties to them,[126] and third states that give consent to assumption of the obligations or rights provided therein.[127] This emphasises the need for consensus, in order for a treaty to have sufficiently broad effect, and to minimise state reservations.[128] Thus, a separate treaty on cyber-attacks would need to ensure sufficient scope of ratification in order to have useful force. Alternatively, the UN Charter could be interpreted to include cyber-attacks. This is consistent with the ICJ's ruling that international instruments must be "interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation".[129] This ascribes to the principle of dynamic interpretation, as provided for under Article 31(3)(b) of the Vienna Convention on the Law of Treaties 1969. Accordingly, the terms 'armed attack' and 'use of force' should be understood in light of technological developments. As has been identified in previous sections, it is possible to interpret the principles of armed attack and the use of force within the cyber context.[130] However, as has also been previously identified, there are several difficulties surrounding such an approach, ranging

---

124 Anna Osula, Agnes Kasper and Aleksi Kajander, 'EU Common Position on International Law and Cyberspace' (2022) 16 *Masaryk University Journal of Law and Technology* 89, 99.

125 Heather Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 *Israel Law Review* 39, 44.

126 Antonio Cassese, *International Law* (2nd edn, OUP 2005) 171.

127 Vienna Convention on the Law of Treaties of 1969, Articles 35-36.

128 Cassese (n 127) 173.

129 *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 Reports 1971, para. 53.

130 Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfections of International Law* (Brill 2015) 4.

from the lack of international consensus on definitions to varied perceptions of threats that cyber-attacks pose.

The existence of such difficulties supports the development of a new, distinct international legal instrument that seeks to promote international consensus on the various aspects of the regulation of cyber operations. This could involve a two-dimensional exercise, whereby existing laws are extended to apply to this new context where possible, and new legal principles are established to fill cyber-related gaps and issues that plague existing law.[131] Such a development is necessary, given the increase in cyber operations, which highlights the need to arrive at an agreement as to the regulation of such operations. This could then form the basis for a binding international instrument. Thus far, debates have resulted in the emergence of general agreement on certain issues, and how they should be regulated under international law. Therefore, there is sound basis for further promotion of such agreement, for the purpose of enacting a legally binding instrument for cyber operations.

A. Cyber Operations as Use of Force and Armed Attacks: Different Approaches

A key issue is to determine how the concepts of use of force and armed attack apply to cyber-attacks. The target-based approach requires that a cyber-attack target national critical infrastructures to amount to a use of force.[132] It does not attach significance to the effects of the attack, so long as it is directed against a national critical infrastructure. This approach is unsatisfactory, because it is far too broad, and would categorise cyber operations as a use of force even in the event that they merely inconvenience, or gather information from, the target state.[133] Furthermore, there is no general consensus on the definition of 'critical national infrastructure', which could give rise to different practices between states. While the target-based approach has the advantage of easily determining whether a cyber operation amounts to a use of force or an armed attack, it fails to respond to the complexity of cyber operations.

The instrument-based approach has traditionally been applied to the regulation of armed force under the UN Charter.[134] It places focus on the means used to

---

131 Noah Simmons, 'A Brave New World: Applying International Law of War to Cyber-Attacks' (2014) 4 *Journal of Law & Cyber Warfare* 42, 48.

132 Russell Buchan and Iñaki Navarrete, 'Cyber Espionage and International Law' in *Research Handbook on International Law and Cyberspace* (Nicholas Tsagourias & Russell Buchan eds, Edward Elgar Publishing 2021) 236.

133 Ibid.

134 Michael Schmitt, 'Computer network attack and the use of force in international law: Thoughts on a normative framework' in *The Use of Force in International Law* (T Gazzini ed, Routledge 2017) 409.

commit the act, but it does not harmonise well with cyber operations, because it focuses on physical means, meaning that a malicious code could not qualify as a use of force. The instrument-based approach has been heavily criticised on the basis that it does not permit cyber operations to be identified as a use of force for the purposes of Article 2(4) of the UN Charter. While the instrument-based approach has the advantage of simplicity, it does not place focus on the consequences of operations.

The most effective approach is the effects-based approach, primarily because it recognises that states are concerned with the consequences of cyber operations than the nature of the weapon or target.[135] It is for this reason that it has received the greatest support of the three approaches. The US has indeed recognised that the international community is primarily focused on the consequences rather than the mechanism of cyber-attacks.[136] The effects-based approach may be applied to identify cyber operations that are comparable to other actions that would be defined as a use of force by the international community.[137] This approach, if embodied within an international instrument, would therefore be most likely to garner international support.

Applying the effects-based approach to cyber operations is not without its difficulties. This is because cyber operations have various consequences, that can range from mere inconvenience to the injury or death of persons, and the damage and destruction of property.[138] Thus, a boundary must be placed between political or economic coercion, and the use of force that reaches the threshold of an armed attack. It has been widely agreed that a cyber operation must have a destructive effect on property and/or persons in order to reach the threshold of armed force.[139] What is apparent is that by placing focus on the consequences, cyber operations can fit more effectively within the current international legal framework. This is also consistent with Rule 69 of the Manual, which adopts a scale and effects approach.

This gives rise to the question concerning how cyber operations that do not directly cause the death or injury of persons and/or the damage or destruction

---

135 Reese Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 *Calif. L. Rev.* 1079, 1121.

136 US Department of Defense, *An Assessment of International Legal Issues in Information Operations* (FAS 1999) 18.

137 Manual, Tule 9.13.

138 Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' in *The Use of Force in International Law* (Tarcisio Gazzini ed, Routledge 2017) 412.

139 Harold Koh, 'International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012' (2012) *Harvard International Law Journal Online* 54, 4.

of property (particularly big data attacks) fit in with this approach. In this respect, Schmitt's development of factors that contribute to assessments of the scale and effects of cyber operations that are indirect and non-physical could apply.[140] These factors are: Severity, directness, immediacy, measurability, invasiveness, military character, state involvement, and presumptive legitimacy. It is beyond the scope of this study to examine these factors in detail, although it is important to point out that they provide a suitable basis for such analysis, as is demonstrated in the fact that they are also provided for in the Manual.[141] They have the effect of distinguishing between cyber operations that do and do not amount to armed force, by way of the fact that they inflict a minimum threshold of harm, their consequences are more imminent and direct than other types of coercion, they are more invasive than other exploitation-based cyber operations, and they have consequences that the international community seeks to avoid. Finally, the level of state involvement is sufficient for the cyber operations to be attributed to it. These factors provide for useful guidance on the categorisation of cyber operations that do not cause direct death or injury or damage or destruction of property.

B. The Application of Existing Laws or a New Law?

There is debate surrounding whether existing law is appropriate in its application to cyber operations, or whether a new international law should be drafted. It is broadly agreed that article 2(4) of the UN Charter and customary international law can be applied to cyber operations, and "must be cast in terms of the use of force paradigm".[142] The term 'armed force' in the UN Charter was intended to be an evolutionary term. Therefore, the fact that cyber operations are not conducted by traditional means is not an insurmountable obstacle to their regulation under the existing framework.[143] Furthermore, there is no evidence to suggest that a completely new international law would avoid the challenges and issues that currently exist. Therefore, a more appropriate approach would be to extend the existing framework, and clarify its application to cyber operations, as the Manual has contributed to achieving. This would also avoid foreseeable issues surrounding the attempt to achieve state ratification of a completely new legal instrument.

---

140 Michael Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 *Vill. L. Rev.* 569, 572.

141 Manual, Rule 69.9.

142 Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' in *The Use of Force in International Law* (Tarcisio Gazzini ed, Routledge 2017) 413.

143 Scott Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkeley J. Int'l Law* 192, 195.

There is general agreement that Articles 2(4) and 51 of the UN Charter are applicable to "any use of force, regardless of the weapon employed", which renders the idea of a completely new international instrument redundant.[144] In previous sections, it has been demonstrated that the UN Charter is able to encompass cyber operations, just as it has applied to other forms of force, such as "kinetic, chemical, biological or nuclear weaponry".[145] This does not mean, however, that challenges and gaps do not exist. This is particularly apparent in the context of where certain forms of cyber operations may be placed in terms of the requisite threshold of armed force. As Melzer points out, cyber operations (particularly those that do not cause death, injury, or destruction) "simply were not anticipated by the drafters of the UN Charter", because they fall within "the grey zone between traditional military force and other forms of coercion".[146] This highlights the need to determine how the existing legal framework should be applied within this context. Arguably, this can only be meaningfully achieved in practice, and when such events occur. At the very least, the basic requirements and thresholds are applicable to cyber operations, in that they must be attributable to a state, amount to a threat or use of force, and be conducted between states. These criteria operate to place limits on the ability to classify cyber operations as a use of force, without becoming overly restrictive or lax. Lingering details should be resolved as practical issues arise, given that there currently exists a very robust basis for the regulation of cyber operations. In contrast, drafting a completely new international regulation would either (a) give rise to new criteria that could give rise to new interpretational problems, or (b) simply emerge as a reiteration of the current law in order to avoid such problems, thereby rendering the legal instrument itself redundant.

CONCLUSION

The first conclusion is that the criteria for the use of force, armed attack, and self-defence can be extended to apply to cyber operations. The Manual has contributed significantly to clarifying the application of key legal principles to the cyber context. The Manual adopts an effects-based rather than an instrument-based approach, reflecting the widely held view that the use of force should be separate from the instrument used. This dismantles boundaries to the application of existing international law to cyber-attacks. Therefore, any use of force that has harmful effects in the form of human injury/death and/or physical damage equivalent to those resulting from military force are in violation of the prohibition, which includes cyber force. This generally excludes big data attacks, depending

144 *Nuclear Weapons Case*, para. 39.

145 Nils Melzer, *Cyberwarfare and International Law* (Policy Commons 2011) 7.

146 Ibid., 9.

on their scale and effects, which is justifiable, given the implications arising from a determination of a use of force. This is supported by the fact that the Manual implies that political or economic coercion is to be excluded from the definition of force. However, this does not mean that cyber operations that have a serious impact on critical infrastructure do not qualify as a use of force, which leaves open the potential for big data attacks to qualify as a use of force. The imposition of such strict boundaries is consistent with the general scope and content of the law on the use of force.

The second conclusion is that big data attacks will rarely meet the necessary threshold, particularly when they merely result in economic damage. It is argued that this is an appropriate approach, given the implications of the qualification of a cyber operation as a use of force. When such attacks result in the injury or death of persons, and/or the destruction of property, only then is it acceptable to define them as a use of force, lest the scope and meaning of the use of force become distorted. This does not mean that big data attacks would never amount to a use of force. The precise reason for the threshold is that an act must meet minimum standards in order to qualify as a use of force. The severity criterion measures the range of consequences of an attack, including but not limited to physical consequences. Therefore, cyber operations that have severe consequences for critical infrastructure may qualify as a use of force, regardless of whether physical damage was caused. Big data attacks, when they only result in economic damage, do not, and should not reach the threshold of the use of force. Accordingly, states should not be permitted to exercise force in self-defence against such attacks. However, if economic damage is accompanied by injury or death, or destruction of property, the right of self-defence may be exercised, provided the requirements are met.

The final conclusion is that, while the Manual (and international law) is plagued by gaps in its application to cyber-attacks, this does not mean that a new international legal instrument would remedy such problems. While international law primarily regulates big data attacks as part of armed conflict, and economic damage is not actionable outside of this context, this is a necessary limitation on the scope of the use of force in self-defence. To allow a big data attack that does not have immediate physical consequences to trigger an armed conflict cannot be reconciled with the foundations of the law on armed conflict. Thus, legislating for this in a separate instrument would conflict with existing law. This highlights the need to determine how the existing legal framework should be applied within this context. Arguably, this can only be meaningfully achieved in practice, and when such events occur. At the very least, the basic requirements and thresholds are applicable to cyber operations, in that they must be attributable to a state, amount to a threat or use of force, and be conducted between states. These criteria operate to place limits on the ability to classify cyber operations

as a use of force, without becoming overly restrictive or lax. Lingering details should be resolved as practical issues arise, given that there currently exists a very robust basis for the regulation of cyber operations.

BIBLIOGRAPHY

Books & Journals

Barkham J, 'Information Warfare and International Law on the Use of Force' (2001) 34 *NYUJ Int'l L. & Pol.* 57

Batinga J, 'Reconciling the Global North-South Divide on the Use of Force: Economic Coercion and the Evolving Interpretation of Article 2(4)' (2024) 41 *Wis. Int'l LJ* 103

Bell AM, 'Using Force against the Weapons of the Weak: Examining a Chemical-Biological Weapons Usage Criterion for Unilateral Humanitarian Intervention under the Responsibility to Protect' (2013) 22 *Cardozo J. Int'l & Comp. L.* 261

Boer LJ, 'Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace' (2013) 5 *Amsterdam LR* 4

Brunnee J, 'The Security Council and Self-Defence: Which Way to Global Security?' in *The Security Council and the Use of Force* (N Blokker & N Schrijver eds, OUP 2005)

Buchan R and I Navarrete, 'Cyber espionage and international law' in *Research handbook on international law and cyberspace* (N Tsagourias & R Buchan eds, Edward Elgar Publishing 2021)

Cassese A, *International Law* (2nd edn, OUP 2005)

Check T, 'The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure' (2022) 13 *Nat'l Sec. L. Brief* 1

Clark, D & S Landau, 'Untangling Attribution' in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (National Research Council 2010)

Coco A, T Dias and T Van Benthem, 'Illegal: The SolarWinds hack under international law' (2022) 33 *European Journal of International Law* 1275

Constantinou A, *The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter* (Sakkoulas 2000)

Corn G & E Jensen, 'The use of force and cyber countermeasures' (2018) 32 *Temp. Int'l & Comp. LJ* 127

Derian-Toth G, R Walsh, A Sergueeva, E Kim, A Coon, H Hadan & J Stancombe, 'Opportunities for public and private attribution of cyber operations' (2021) 12 *Tallinn Paper Series* 8

Devins C, T Felin, S Kauffman, R Koppl, 'The Law and Big Data' (2017) 27 *Cornell Journal of Law and Public Policy* 363

Dinniss HH, *Cyber Warfare and the Laws of War* (CUP 2012)

Dinniss HH, 'The nature of objects: Targeting networks and the challenge of defining cyber military objectives' (2015) 48 *Israel Law Review* 39

Dinstein Y, *War, Aggression and Self-Defence* (CUP 2010)

Dobinson I & F Johns, 'Legal research as qualitative research' in *Research methods for law* (M McConville & WH Chui eds, 2nd edn, Edinburgh University Press 2017)

Efrony D & Y Shany, 'A rule book on the shelf? Tallinn manual 2.0 on cyberoperations and subsequent state practice' (2018) 112 *American Journal of International Law* 583

Eichensehr KE, 'Not illegal: The SolarWinds incident and international law' (2022) 33 *European Journal of International Law* 1263

Focarelli C, 'Self-defence in cyberspace' in *Research handbook on international law and cyberspace* (N Tsagourias & R Buchan eds, Edward Elgar Publishing 2021)

Foltz A, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate' (2012) 67 *Joint Force Quarterly* 40

Gill TD, 'The temporal dimension of self-defence: Anticipation, pre-emption, prevention and immediacy' (2006) 11 *Journal of Conflict and Security Law* 361

Green JA, 'The ratione temporis elements of self-defence' (2015) 2 *Journal on the Use of Force and International Law* 97

Gunatileka S, '"Big Data Breaches", sovereignty of states and the challenges in attribution' (2024) 5 *University of Colombo Review* 104

Hayward RJ, 'Evaluating the Imminence of a Cyber Attack for Purposes of Anticipatory Self-Defence' (2017) 117 *Colum. L. Rev.* 399

Hernandez G, *International Law* (OUP 2019)

Hollis DB & TJ Van Benthem, *Threatening Force in Cyberspace* (Temple University Legal Studies Research Paper 2021)

Jensen ET, 'Computer attacks on critical national infrastructure: A use of force invoking the right of self-defence' (2002) 38 *Stan. J. Int'l L.* 207

Kilovaty I, 'Attacking Big Data as a Use of Force' *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (L Dickinson & E Berg eds, Vol. 9, OUP 2024)

Koh H, 'International Law in Cyberspace: Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012' (2012) *Harvard International Law Journal Online* 54

Kretzmer D, 'The inherent right to self-defence and proportionality in jus ad bellum' (2013) 24 *European Journal of International Law* 235

Kumar D, 'Interpretation of International Law under the Tallinn Manual(s)' (2021) 3 *Indian JL & Legal Rsch.* 1

Lavania A, 'The Need to Fill Legal Vacuum in International Law to Deal with Non-State Actors in Cyber Operations' (2022) 5 *Int'l JL Mgmt. & Human.* 462

Lin HS, 'Offensive cyber operations and the use of force' (2010) 4 *J. Nat'l Sec. L. & Pol'y* 63

Lubell N, *Extraterritorial Use of Force Against Non-State Actors* (OUP 2010)

Marelli M, 'The SolarWinds hack: Lessons for international humanitarian organizations' (2022) 104 *International Review of the Red Cross* 1267

Melzer N, *Cyberwarfare and International Law* (Policy Commons 2011)

Motoyoshi Y, 'The Legal Framework of the 'Unwilling or Unable' Theory and the Right of Self-Defence against Non-State Actors' (2021) 37 *Nihon University Comparative Law* 25

Nguyen R, 'Navigating jus ad bellum in the age of cyber warfare' (2013) 101 *Calif. L. Rev.* 1079

O'Meara C, *Necessity and Proportionality and the Right of Self-defence in International Law* (OUP 2021)

Osula AM, A Kasper & A Kajander, 'EU common position on international law and cyberspace' (2022) 16 *Masaryk University Journal of Law and Technology* 89

Palleti VR, S Adepu, V Mishra & A Mathur, 'Cascading effects of cyber-attacks on interconnected critical infrastructure' (2021) 4 *Cybersecurity* 1

Pipyros K, C Thraskias, L Mitrou, D Gritzalis & T Apostolopoulos, 'A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual' (2018) 74 *Computers & Security* 371

Pradeep MD, 'Legal Research-Descriptive Analysis on Doctrinal Methodology' (2019) 4 *International Journal of Management, Technology and Social Sciences* 95

Radziwill Y, *Cyber-attacks and the exploitable imperfections of international law* (Brill 2015)

Reyes P, 'Self-Defence against Non-State Actors: Possibility or reality?' (2021) 9 *Revista Facultad de Jurisprudencia* 151

Roscini M, 'Threats of armed force and contemporary international law' (2007) 54 *Netherlands International Law Review* 229

Roscini M, *Cyber operations and the use of force in international law* (OUP 2014)

Schmitt MN, 'Cyber operations and the jud ad bellum revisited' (2011) 56 *Vill. L. Rev.* 569

Schmitt MN, 'The notion of 'objects' during cyber operations: A riposte in defence of interpretive and applicative precision' (2015) 48 *Israel Law Review* 81

Schmitt MN, 'Computer network attack and the use of force in international law: Thoughts on a normative framework' in *The Use of Force in International Law* (T Gazzini ed, Routledge 2017)

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017)

Schmitt MN, 'Big Data: International Law Issues Below the Armed Conflict Threshold' in *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (L Dickinson & E Berg eds, Vol. 9, OUP 2024)

Schmitt MN & S Watts, 'Beyond state-centrism: International law and non-state actors in cyberspace' (2016) 21 *Journal of Conflict and Security Law* 595

Shackelford SJ, 'From nuclear war to net war: Analogizing cyber attacks in international law' (2009) 27 *Berkeley J. Int'l Law* 192

Shaw MM, *International Law* (7th edn, CUP 2014)

Simma B, DE Khan, G Nolte & A Paulus, *The Charter of the United Nations: A Commentary* (4th edn, OUP 2024)

Simmons N, 'A Brave New World: Applying International Law of War to Cyber-Attacks' (2014) 4 *Journal of Law & Cyber Warfare* 42

Stahn C, 'Terrorist Acts as Armed Attack: The Right to Self-Defense, Article 51 (½) of the UN Charter, and International Terrorism' (2003) 27 *The Fletcher Forum of World Affairs* 35

Symon P, A Tarapore, 'Defense Intelligence Analysis in the Age of Big Data' (2015) 79 *Joint Force Quarterly* 5

Tsagourias N, 'Non-State Actors and the Use of Force' in *Participants in the International Legal System: Theoretical Perspectives* (J D'Aspremont ed, Routledge 2011)

Tsagourias N, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' (2012) 15 *Yearbook of International Humanitarian Law* 19

Tsagourias N, 'Cyber attacks, self-defence and the problem of attribution' (2012) 17 *Journal of Conflict and Security Law* 229

Uniacke S, 'The condition of last resort' in *The Cambridge handbook of the just war* (L May ed, CUP 2018)

Withers P, 'Do we need an effects-based approach for cyber operations?' in *Research Handbook on Cyberwarfare* (T Stevens & J Devanny eds, Edward Elgar Publishing 2024)

Yoo J, 'Using force' (2004) 71 *University of Chicago Law Review* 729

Ziolkowski K, *Stuxnet: Legal considerations* (NATO Cooperative Cyber Defence Centre of Excellence 2012)

Reports

International Criminal Court, *Report of the Special Working Group on the Crime of Aggression*, ICC-ASP/7/ SWGCA/2 (2009)

US Department of Defense, *An Assessment of International Legal Issues in Information Operations* (FAS 1999)

Resolutions

United Nations Security Council (UNSC) Res 1373 (28 September 2001) UN Doc S/RES/1373

United Nations Security Council (UNSC) Res 1368 (12 September 2001) UN Doc S/RES/1368

Judgements

Armed Activities on the Territory of the Congo (Dem. Rep. Congo v Rwanda) (2006) ICJ 6

Bosnia and Herzegovina v Serbia and Montenegro (2007) ICJ 2

Caroline v United States, 11 U.S. 496 (1813)

Gabcikovo-Nagymaros Project (*Hungary v Slovakia*) (1997) ICJ 692

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 Reports 1971

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (2004) ICJ Rep 28

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA) (1986) ICJ Rep 14

Oil Platforms Case (Islamic Republic of Iran v United States of America) (2003) ICJ Rep 4

Prosecutor v Dusko Tadic (1999) ICTY Appeals Chamber, IT-94-1-A

Law

Charter of the United Nations 1945

Declaration on Friendly Relations 1970

Vienna Convention on the Law of Treaties 1969