UCHE OKEREKE-FISHER *Barrister-at-Law*

STATE CHAMBERS, LEVEL 36, 52 MARTIN PLACE, SYDNEY NSW 2000; TEL: 0423018344; EMAIL: ufisher@statechambers.net

THE REGULATION OF AUSTRALIA'S RESPONSE TO CYBER ATTACKS

A. ABSTRACT

The malicious hack and release of sensitive information from the US Democratic National Committee by Russian cyber operatives in the 2016 US Presidential election brought to the fore the growing use of malicious information technology by rogue nations and organized criminal groups. The operation demonstrated to the world the real potential for information in cyberspace to be manipulated and the ability of foreign states to wrongfully interfere with processes underpinning the democracy of a sovereign state. The interference evinced unacceptable behaviour in cyberspace and tested concepts around attribution, response and effective deterrence.

This paper examines the laws, policies and strategies that govern and regulate Australia's response to a state-sponsored cyber attack. The paper outlines definitions of a cyber attack. It provides insights into existing international laws, domestic policy and strategies that regulate Australia's activities in cyberspace within the constraints of the legal framework. It then examines the nature of a cyber attack that qualifies as state-sponsored, a cyber operation that constitutes a "use of force" and/or "armed attack". It also explores the legal framework that governs the extent to which Australia can rely on *jus ad bellum* and the constraints of international laws. Consequently, the following questions arise - (i) What is a cyber attack?; (ii) When is a cyber attack, State-sponsored?; (iii) At what point does a cyber attack escalate to an act of war or "armed attack"?; (iv) When is a cyber operation tantamount to the "use of force"?; and (v) What are the international laws applicable to cyber warfare?

B. INTRODUCTION

Cyberspace has become an increasingly important domain, woven intricately into our trade and commerce, businesses, critical infrastructures and our daily existence[1]. Today, computer technology is at the heart of all we do. Australia's critical infrastructures are increasingly dependent on computers and computer services. However, this overwhelming reliance on cyberspace exposes our society to the vulnerabilities associated with technology. The more technologically advanced a state is, the more vulnerable it is to cyber attacks. If computer networks become the "nerve system" of civilian and military infrastructures, disrupting them will be tantamount to paralyzing the country[2].

Hostile activity in cyberspace has the potential to threaten international peace, security and stability. A large-scale cyber attack on critical infrastructure would have severe implications for international security[3]. The most harmful attacks using information technology include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful attacks against critical infrastructure is both real and serious[4]. The borderless nature of cyberspace means that the capacity and behaviour of other states, the private sector, civil society and individuals can affect Australia's cyber interests[5]. Advanced malicious cyber activity

---

[1] Australia's Cyber Security Strategy, First Annual Update, <www.cybersecuritystrategy.pmc.gov.au/cyber-security-strategy-first-annual-update-2017.pdf> at 9.

[2] The United States National Security Strategy recalls that "the very technologies that empower us to lead and create also empower those who would disrupt and destroy", National Security Strategy, May 2010, 27<www.whitehouse.gov/default/files/rss_vewer/national_security_strategy.pdf>.

[3] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, October 2017, at 45.

[4] United Nations report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, at 8.

[5] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy, October 2017*, at 83.

against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity. The reach and diversity of cyber adversaries are expanding, and their operations against both government and private networks are constantly evolving[6].

The Australian Cyber Security Center (**ACSC**) continues to assess that a cyber attack against Australia would most likely be aimed at high value targets such as critical infrastructure, government networks or military capabilities. Over the last 12 months, the ACSC has detected extensive state-sponsored activity against Australian government and private sector networks in support of economic, foreign policy and national security objectives[7]. The foregoing notwithstanding, Australia has not been subjected to hostile cyber activity that would constitute an official cyber attack.

Although Australians and Australian interests are routinely targeted for compromise, no adversary has sought to disrupt or degrade Australian networks, or misuse stolen data to achieve the serious compromise of national security, stability or economic prosperity that would be considered to be a cyber attack[8].

Commentators have suggested that the pandemonium created by the cyber mania is exaggerated. They claim that the vast majority of cyber-attacks are not carried out by government-sponsored hackers but by criminals intending to steal business secrets and financial information. They argue that analogising cyber attack incidents to war defeats the purpose of making the internet accessible and secure and is detrimental

---

[6] *Australian Cyber Security Center, Threat* Report 2017, at 16: <www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf>.

[7] *ibid* at 16.

[8] *ibid* at 50.

to preventing the real challenges to cyber security, crime and espionage[9].

C. DEFINITION OF CYBER ATTACK

Literature review of articles by legal scholars in this field reveals a startling lack of consensus on the use of terms like cyber war, cyber attack, cyber warfare and cyber terror. Generally, these terms are used to describe conducts or activities that undermine or compromise the function of a computer network for a malicious purpose.

Cyber attack has been defined as (i) 'efforts to alter, disrupt or destroy computer systems or networks or the information or programs on them; and (ii) 'deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks'[10]. The Australian Government defines "cyber attack" as a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity[11]. Likewise, cyber terrorism has been defined as "unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives"[12].

For the purpose of this essay, a cyber attack is a cyber operation, whether offensive

---

[9] Mary O'Connell, Louise Ariatsu, Elizabeth Wilmhurst, Chatam House, International Law Meeting Summary, 29 May 2012 *Cyber Security and International Law*, at 3.

[10] Matthew C. Waxman, "Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)", 36 *Yale Journal of International Law* (2011), 422.

[11] Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy, October 2017, at 47.

[12] Professor Denning D in testimony before the US House of Representatives Committee on Armed Services, Special Oversight Panel on Terrorism, 23 May 2000, as cited in Grabosky P and Stohl M 'Cyber-terrorism' (2003) 82 *Reform* at 8.

or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects[13].

The law of armed conflict applies to the targeting of any person or object during armed conflict irrespective of the means or methods of warfare employed. “Attack” means an act of violence against the adversary, whether in offence or defence. Hence, it is the use of violence that distinguishes an “attack” from other military operations. The better view is that non-violent operations such as psychological cyber operations and cyber espionage do not qualify as attacks[14]. Notably, however, acts of violence are not limited to activities that release kinetic force. Chemical, biological and radiological attacks qualify as acts of violence. The consequences of an operation, not its nature, is what determines the scope of the term “attack”. The word “cause” is not limited to the effects on the targeted cyber system, but extends to any reasonably foreseeable consequential damage, destruction, injury or death.

The definition of cyber attack extends to an attack on data where the attack foreseeably results in the injury or death or death of individuals or damage or destruction of physical objects. The United Nations International Group of Experts agrees that not all cyber operations qualify as attack[15]. For example, the disruption of all email communications in the country (as opposed to the damaging the system on which the transmission relies) may have large-scale adverse consequences, but the law of armed conflict would not apply. Experts agree that cyber operations that merely

---

[13] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations,* Rule 92, at 415; this is consistent with the decision of the International Court of Justice in *Legality of the Threat or Use of Nuclear Weapons* [1996] ICJ 2 which decided that the means of attack is immaterial to its classification (at note 8, paragraph 39).

[14] *Ibid* at 415.

[15] *Ibid* at 418.

cause inconvenience or irritation to the civilian population do not rise to the level of attack. Notably, a cyber operation need not result in the intended destructive effect to qualify as an attack.[16] Hence, an attack that is successfully intercepted and does not result in actual harm is still an attack under the law of armed conflict, if absent the interception, it would have been likely to cause the intended consequences[17]. Not all cyber incidents therefore constitute a cyber attack, and not all cyber attacks constitute an act of cyber war.

In March 2011, the US Defense Department admitted that it was a victim to a cyber-espionage leaks, where foreign hackers gained access to over 24,000 Pentagon files[18]. The Distributed Denial of Service attack on US Domain Name System provider, Dyn, disrupted major internet platforms and services in Australia, Europe and North America revealing vulnerabilities in Australia's internet infrastructure. In Australia, the eCensus failure highlighted the flaws in the government's digital transformation agenda. Although all of these incidents compromised the security of a computer network for the purpose of carrying out a military objective, they do not meet this paper's definition of a cyber-attack.

Mere cyber-espionage, or cyber-exploitation, does not constitute a cyber-attack, because neither of these concepts involves altering computer networks in a way that affects their current or future ability to function[19]. Undermining the function of a computer system requires conduct that affects the operation of the system either by damaging the operating system or by adding false, misleading, or unwelcome

---

[16] *Ibid* at 419 ("*AMW MANUAL, Commentary to Rule 1(e)*").

[17] *Ibid* at 419.

[18] Thom Shanker & Elisabeth Bumiller, *Hackers Gained Access to Sensitive Military Files*, NY Times at A6, July 15, 2011.

[19] Oona A.Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, "The Law of Cyber-Attack", *California Law Review*, 2012 at 14.

information. Such activities may be criminal - as acts of corporate or political cyber-espionage - but are not cyber-attacks.

When is a cyber attack state-sponsored?

A cyber attack is State-sponsored if it is authorised by a state and can be attributed to the relevant state. Article 8 of the International Law Commission Articles provides that "*the conduct of a person or group of persons shall be considered an act of a state under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct".*

In the event of a cyber attack on Australian interests or critical infrastructure in cyberspace, the paramount issue that will emerge is the issue of identifying the source of the cyber attack and attributing the attack to the perpetrators or the Offending State. Given the possibility of retaliation by Australia and the attendant consequences of such conduct, it would be imperative that Australia identifies with precision and without doubt, the identity of the Offending State. Therein lies the quagmire. Origin of cyber attacks can be disguised by IP spoofing or the use of botnets. Anonymity is in fact one of the greatest advantages of cyberwarfare: even though the attacks might appear to originate from computers located in a certain country, this does not necessarily mean that the country or the owners of the computers involved were behind such actions[20]. The actors' conduct will be imputable to the State of which they are *de jure* organs[21].

[20] Marco Roscini, "World Wide Warfare- Jus ad bellum and the Use of Cyber Force" *Max Planck Yearbook of United Nations Law*, Volume 14, 2010 at 99.

[21] According to Article 4 of the 2001 ILC Articles on State responsibility, "*the conduct of any state organ shall be considered act of that State under international law whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State and whatever character as an organ of the central government or of a territorial unit of the State".*

Another complication associated with identification and attribution is the fact that details of state military capabilities are not publically available. Also, the perpetrator may not be a state. It may be members of government agencies, private corporations or independent contractors not acting under the authority of a state. Nevertheless, the relevant cyberattack will be attributed to the state "provided the person or entity is acting in that capacity in that particular instance[22].

Identification and attribution may prove insurmountable in certain cases. For example, the widely reported cyber attack on the Estonia government. The Cyberattack was in response to the moving of a soviet war memorial; hackers interfered with the Estonia government websites using distributed denial of service. Though these attacks were widely believed to have been executed by Russia, the true identity of the perpetrators was never authenticated. Some argued that Estonia was attacked in a way that triggered the North Atlantic Treaty's (NATO) Article 5. However, NATO did not respond with a counter-attack but it did establish an internet defence facility in Estonia called the Cooperative Cyber Defense Center of Excellence (CCDCOE)[23].

When is a Cyber attack an act of war?

The United Kingdom Under-Secretary for security and counter-terrorism also declared that a cyber attack that took out a power station would be an act of war[24]. In his remarks on the new White House cyber security office, President Obama qualified

[22] Point 61, page 99, CA2 ILC Articles on State Responsibility, article 5, see note 52.

[23] Mary O'Connell, Louise Ariatsu, Elizabeth Wilmhurst, Chatam House, International Law Meeting Summary, 29 May 2012 *Cyber Security and International Law*, at page 4.

[24] J. Doward, "*Britain fends off flood of foreign cyber-attacks*", The Observer, 7 March 2010,19.

attacks on defence and military networks as a "weapon of mass disruption[25]. This paper argues that a Cyber attack, which triggers the self-dense right in Article 51 of the UN Charter, would be deemed to be an act of war.

D. INTERNATIONAL LAW AND RESPONSE TO CYBERATTACK

A state-sponsored cyber attack on Australia will raise the question of what remedies are available to Australia as the victim state. The nature and scope of Australia's response to a cyber attack will be subject to International law. The International Court of Justice has stated that Articles 2(4) and 51 of the United Nations Charter regarding the prohibition of the use of force and self-defense respectively apply to any "use of force" regardless of the weapons employed[26]. With respect to cyber operations, it is not the instrument used that determines whether the use of force threshold has been crossed but rather, the consequences of the operation and its surrounding circumstances[27].

When attributed to a state successfully, a cyber attack is a violation of the customary principle of non-intervention "on matters in which each state is permitted, by the principle of State sovereignty, to decide freely" such as "the choice of a political, economic, social and cultural system and formulation of foreign policy[28]. Hence, Cyber attacks can also amount to an unlawful intervention. For example, where a state

---

[25] "Remarks on securing the nation's cyber infrastructure", see note 1.

[26] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations,* Rule 92, at 328.

[27] *Ibid.*

[28] ICJ reports 1986, see note 64, 107 et seq. (para.205). The principle of non-intervention has been reported in a number of agreements, but it is not expressly stated in the UN Charter. According to the ICJ, however, the principle is "part and parcel of customary international law" (*ibid*, 106, para 202).

engages in cyber propaganda through the defacement of websites aimed at formenting civil strife in the target state or sending of thousands of emails to voters in order to influence the outcome of political elections in another state[29].

Use of Force and Armed Attack

Legal regulation of the use of force begins with Article 2(4) of the United Nations (UN) Charter. Article 2(4) of the UN charter states that "*all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*."[30] Article 51 of the Charter then provides that "*nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations*".

This section examines the norms of *jus ad bellum* as they presently exist[31]. 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[32]. There are two exceptions to the prohibition of the use of force – use of force authorized by the Security council under Chapter VII and self-defense pursuant to Article 51.

---

[29] See para II(j) of the Declaration on Non-Intervention.

[30] UN Charter article 2, para 4.

[31] *Jus ad bellum* is the criteria that are to be referred to before engaging in war in order to determine whether it is justifiable. *Jus in bello* is the law that governs the manner in which warfare is conducted.

[32] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations*, Rule 68, at 329.

Art 2(4) contains two prohibitions – the prohibition against the use of threat and the prohibition against the use of force. There is no authoritative definition of the terms "threat" and "use of force". The UN Charter does not stipulate a criterion to determine whether an act amounts to a use of force.

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[33]. The notion of "use of force" should be considered in relation to an "armed attack" which is the threshold at which a state may lawfully use force in self-defense. In the Nicaragua judgment[34], the ICJ found that "scale and effects" are to be considered when determining whether particular actions amount to an "armed attack"[35]. This same test applies to what constitutes "use of force". In the same case, the ICJ distinguished the most grave forms of the "use of force" (*those constituting an armed attack for the purposes the law of self-defense*) from other less grave forms[36]. In *Nicaragua v US*, the Court noted that merely funding guerrillas engaged in operations against another state did not cross the use of force threshold. However, it found that arming and training a guerrilla force that is engaged in hostilities against another state qualifies as a use of force. Hence, "use of force' is not restricted to the employment of the offending State's own military or armed forces.

---

[33] *Ibid* at 330.

[34] *Military and Paramilitary Activities in and Against Nicaragua* (1986) I.C.J. 14 (27 June) (***Nicaragua v US***); and see also at [202] ("The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference. . . . Expressions of an *opinio juris* regarding the existence of this principle ... are numerous .... .").

[35] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations,* Rule 71, at 339.

[36] *Nicaragua v US*, para 191. The court pointed to the Declaration on Friendly Relations, noting that while certain of the actions referred to therein constituted armed attacks, others only qualified as uses of force.

Notably Article 2(4) of the UN Charter does not specify the methods through which a threat could be carried out and thus communicating a threat via Internet would be on the same theoretical footing as communicating a threat by traditional methods. The cyber threat could also warn of a possible cyber attack by the threatening state. Whether this is a threat under Article 2(4) depends on whether the use of cyber force envisaged in the threat is unlawful. The ICJ has linked the legality of threats to the legality of the use of force in the same circumstances. The question is whether the cyber operation constitutes the "use of force" for the purpose of the prohibition in Article 2(4). The prohibition extends to non-Member States by virtue of customary international law. The fact that a cyber operation does not qualify as "use of force" does not necessarily render it lawful under international law. It may constitute a violation of sovereignty[37] or a breach of the prohibition on intervention[38]. "Use of force" and "threat" are not defined under the Charter. However, certain categories of coercive operations do not qualify as "use of force".[39]

Historically, there is a great divide on the interpretation of the prohibition of the use of force in Art 2(4). The prevailing view in the United States is that the prohibition of the use of force in Article 2(4) ("the "Prohibition") and the complementary right of self-defense in Art 51 ("Self-Defense Right") apply solely to military attacks or armed violence.[40] This view is somewhat supported by the textual meaning as seen in the

---

[37] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations,* Rule 4, at 339 ("A State must not conduct cyber operations that violate the sovereignty of another state").

[38] *Ibid* at 312.

[39] Matthew C. Waxman, "The Power to Threaten War", *The Yale Law Journal*, 123:1626, (2014); Matthew C. Waxman, "Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)", 36 *Yale Journal of International Law* (2011), 430.

[40] See NRC Committee Report, *supra* note 4, at 253 ("traditional [law of armed conflict] emphasizes death or physical injury to people and destruction of physical property as criteria for definitions of "use of force" and "armed attack"); Tom J. Farer, "Political and Economic Coercion in Contemporary International Law", 79 *AM. J. INTL'L.* 405, 408-09 (1985) (describing two main interpretations of Articles 2(4) and 51, arguing that the only one wherein "the only justification for force is prior or imminent armed force by one's adversary" is logically sound); Albrecht Randelzhofer, Article 2(4) in "The Charter of the

UN Charter's preamble, which sets out the goal that "*armed force….not be used save in the common interest*". Also, Article 51 refers to self-defense against "armed" attacks. This narrow interpretation of the Prohibition implies that other use of force, for example, via coercion or interference is not caught by Article 2(4).

Pursuant to the narrow interpretation school of thought, an Australian retaliation or response regime that includes interference with the offending State's financial regulatory systems, covert economic disruptions or computer network attacks may not be caught by the Prohibition, to the extent that it does not involve military attacks or armed violence. Furthermore, it is argued that the expression of "force" also appears in the Preamble of the Charter and in Articles 41 and 46 where it is preceded by the adjective "armed" whilst in Article 44, the reference is to military force only[41]. This has enabled the argument that "force" though unqualified in Article 2(4) refers to armed force.

The second school of thought counter-argues that the specification of "armed attacks" in Article 51 suggest that the drafters envisioned the prohibited "force" in Article 2(4) as a broader category not limited to particular methods [42]. This broader interpretation sees coercion as a "use of force". This view is embraced by States in the developing world, which have pushed the notion that force includes other forms of pressure,

---

United Nations: A Commentary", *supra* note 22, at 112, 117 (noting that the term "force" as used in Article 2(4) is "according to the correct and prevailing view, limited to armed force"); Bert V. A. Roling, "*The Ban on the Use of Force and the UN Charted*", The Current Legal Regulation of The Use of Force 3, 3 (A. Cassese ed,1986) ("it seems obvious to the present writer that the "force" referred to in Art 2(4) is "military force").

[41] Article 41 of the UN Charter includes "the complete or partial interruption of [….] telegraphic, radio and other means of communication" in the list of measures "not involving the use of armed force"; this however is not helpful where the effect of the cyber attacks on a computerized society is more drastic than contemplated by the drafters.

[42] Matthew C. Waxman, "Cyber-Attacks and Use of Force: Back to the Future of Article 2(4)", 36 *Yale Journal of International Law* (2011), 428.

including political and economic coercion threatening to state autonomy[43].

Pursuant to the broad interpretation, Australia would be in violation of the Prohibition if the intended response is likely to exert coercive pressure on the victim state – for example by threatening to cripple its financial sector. The question that also arises is whether such a forceful response albeit in the form of economic coercion can trigger the Self-Defense Right in favour of the victim state under Article 51. The broader interpretation proponents argue that if the drafters wanted to refer to "armed force", they would have said so expressly and, as this was not included in Article 2(4), the drafters intended a broad interpretation. However, the *travaux preparatoires* reveal that the drafters did not intend to extend the Prohibition to economic coercion and political pressures[44].

It is therefore generally agreed that Article 51 carves out an exception to the prohibition of the use of force as set out in Art 2(4). However, there is significant debate about the extent to which the self-defense right in Article 51 permits a state to resort to military force. Here, the question that emerges is whether the existing international legal framework imposes constraints on hostile retaliatory cyber operations. Does the self-defense right pursuant to Article 51 give rise to a right to use military force in response?

The classic statement of justification for pre-emptive self defence was issued by U.S. Secretary of State Daniel Webster in 1842 in response to British military claims of justification in attacking the steamboat the *Caroline* in 1837 near Niagara Falls. The

[43] *Ibid* at 429.

[44] According to article 32 of the 1969 Vienna Convention on the Law of Treaties, the preparatory works of a treaty are a supplementary means of interpretation.

boat had been conveying men and arms to fuel a rebellion in Upper Canada. A British military unit entered the United States and destroyed the vessel resulting in the loss of two American lives. The British claimed to be acting in self-defence. Webster's letter to his counterpart, Lord Ashburton, argued:

> "Undoubtedly it is just, that, while it is admitted that exceptions growing out of the great law of self-defense do exist, those exceptions should be confined to cases in which the necessity of that self-defence is instant, overwhelming, leaving no choice of means, and no moment of deliberation".[45]

The British accepted this test by justifying its actions accordingly.[46] The "*Caroline* test" requires that nations show that use of force is necessary due to an imminent threat, and that the response is proportionate to the threat. The test came to be accepted as part of customary international law.[47]

A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects[48]. An armed attack must have a trans-border element. This is achieved when a state engages another state in cyber operations that qualify as an armed attack or when a state directs non-state actors to act on its behalf. The right to employ force in self-defense extends beyond kinetic

---

[45] Letter from U.S. Secretary of State Daniel Webster to British Minister Henry Fox (Apr. 24, 1841), in 29 *British and Foreign State Papers*, 1840-1841, at 1138 (1857).

[46] Letter from Lord Ashburton to U.S. Secretary of State Daniel Webster (July 28, 1842), in 30 *British and Foreign State Papers*, 1841-1842, at 1858 (1857).

[47] John Yoo, "International Law and the War in Iraq" 97 *Am. J. Int'l L.* 563 (2003) at 572.

[48] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations,* Rule 71, at 339.

armed attacks to cyber operations[49]. To qualify as an armed attack, the cyber operation must employ the use of a cyber weapon. An armed attack presupposes the use of force for the purpose of Art 2(4) but it does not equate to use of force. Not every use of force rises to the level of an armed attack[50]. The scale and effects required for an act to be characterized as an armed attack exceed those required to qualify an act as use of force.

The law is still unclear as to the precise point at which the effects of a cyber operation will tantamount to an armed attack. In the *Nicaragua v US* judgment, the ICJ accepted that a definition of "armed attacks" is not included in the Charter and is not part of Treaty Law. However, the Court distinguished between an armed attack and a "mere frontier incident". The ICJ also noted that Article 51 does not refer to specific weapons and that it applies to "any use of force, regardless of the weapons employed".

This paper contends that the fact cyber attacks do not employ the use of traditional weapons does not mean that they are not "armed attacks" and as such exempted from Article 51. As Zemanek notes "*it is neither the designation of a device, nor its normal use which makes it a weapon but the intent with which it is used and its effect*". The use of any device which results in a considerable loss of life and/or extensive destruction of property must therefore qualify as an armed attack[51]. The foregoing notwithstanding, it is acceptable that not all cyber attacks will qualify as an armed attack.

[49] *Ibid* at 340.

[50] *Nicaragua v US* para 191.

[51] K. Zemanek, *"Armed Attack" Max Planck Encyclopedia of Public International Law*, 2010, para 21.

There is also no consensus on the status of cyber operations that do not result in injury, death, damage or destruction but which otherwise have extensive negative effects. This is illustrated in the 2010 Stuxnet operation. Despite the scale of the damage caused to Iranian centrifuge, there is no consensus that this amounted to an armed attack- even though there is an agreement that it constituted use of force[52].

Pursuant to Article 51, Australia as a victim state would have the right to individual or collective self-defense if the relevant attack is characterised as an "armed attack". Thus, in contemplating retaliatory cyber operations, Australia must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition of the use of force[53] and whether the incident qualifies an armed attack to trigger the Self-Defense Right.

In assessing whether its contemplated operations will violate the prohibition in Art 2(4), Australia will consider the following factors: the severity, the immediacy, the directness, the invasiveness, measurability of effects, the military character, and the presumptive legality of State involvement. These factors are not legal criteria and are not exhaustive.

E. AUSTRALIAN REGULATORY FRAMEWORK

Governments routinely engage in a wide spectrum of cyber operations, and researchers have identified more than 100 states with military and intelligence cyber

[52] International Group of Experts at the invitation of NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law applicable to cyber operations*, at 342.

[53] *Ibid* at 333.

units[54]. The Australian government embraces transparency and has declared the existence of its offensive cyber capability and its ability to respond to serious cyber attacks, support military operations, and to counter offshore cybercriminals[55]. In April 2016, Prime Minister Malcolm Turnbull confirmed that Australia has an offensive cyber capability. This was the first time any State had announced such a policy[56]. In November 2016, he announced that the capability was being used to target Islamic State, and on 30 June 2017 Australia became the first country to openly admit that its cyber offensive capabilities would be directed at 'organized offshore cyber criminals'.

Australia's offensive cyber capability resides within the Australian Signals Directorate (ASD). It can be employed directly in military operations, in support of Australian law enforcement activities, or to deter and respond to serious cyber incidents against Australian networks. While physically housed within ASD, the military and law enforcement applications have different chains of command and approvals processes[57]. Any offensive cyber operation in support of the ADF is planned and executed under the direction of the Chief of Joint Operations and, as with any other military capability, is governed by ADF rules of engagement[58].

When the first public disclosure of Australia's offensive cyber capability was made, the Prime Minister emphasized Australia's compliance with international law: '*The use of such a capability is subject to stringent legal oversight and is consistent with our support for the international rules-based order and our obligations under international*

[54] Fergus Hanson and Tom Uren, Australia's Offensive Capability at 5 < www.aspi.org.au/report/australias-offensive-cyber-capability>.

[55] *Ibid.*

[56] *Ibid* at 4.

[57] *Ibid* at 6.

[58] *Ibid* at 7.

law.[59]. Every offensive cyber operation is planned and conducted in accordance with domestic law, and is consistent with Australian obligations under international law[60].

Australia accepts the centrality of international law and its application to States' use of cyberspace was affirmed in 2013 in the consensus report of the third *United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, which was chaired by Australia, and reaffirmed in the 2015 report of the UNGGE. However, Australia recognizes that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders.

Australia's stance can be summarized as follows[61]:

- The United Nations Charter and the law on the use of force (*jus ad bellum*) apply to activities conducted in cyberspace.
- For cyber operations constituting or occurring within the context of an international or non-international armed conflict, the relevant international humanitarian law (*jus in bello*) will apply to the conduct of these cyber activities.
- For cyber activities taking place outside of armed conflict, general principles of international law, including the law on state responsibility, apply.
- Australia also adopts norms that regulate the responsible behaviour of States in

[59] *Ibid* at 6.

[60] *Ibid* at 9.

[61] Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber Engagement Strategy, October 2017, at 90.

cyberspace as reflected in the report of the 2015 *UN Group of Government Experts* on *Development in the Field of Information and Telecommunications in the Context of International Security* (A/70/174)[62].

- The cumulative reports of the *UN Group of Governmental Experts on Developments in the Field of Information and Communication Technologies in the Context of International Security* (UN Group of Governmental Experts) have contributed to our collective understanding of how international law applies to states' conduct in cyberspace. The Tallinn Manuals are also an important academic contribution to international legal dialogue in this area[63].

CONCLUSION

Regulation of cyberspace activities pose unique albeit familiar problems. Legal line drawing with respect to the use of force and right to self-defence reflects the distribution of power and vulnerability amongst States.

In the event of a state-sponsored cyber attack, Australia's response could comprise law enforcement or diplomatic, economic or military measures as appropriate for the circumstances. This could include, but is not restricted to, offensive cyber capabilities that disrupt, deny or degrade the computers or computer networks of adversaries. Regardless of the context, Australia's response would be proportionate to the circumstances of the incident, would comply with domestic law, and be consistent with its obligations under international law.

Attribution of malicious activity is necessary to enable a range of response options.

[62] *Ibid* at 92.

[63] *Ibid* at 48.

Depending on the seriousness and nature of an incident, Australia has the capability to attribute malicious cyber activity in a timely manner to several levels of granularity – ranging from the broad category of adversary through to specific States and individuals. Australia's strong cyber security posture underpins its ability to deter and respond to serious incidents and unacceptable behaviour in cyberspace. It ensures that Australia can discourage, detect, respond to, and contain malicious cyber activity effectively[64].

Uche Okereke-Fisher
Barrister-at-Law
State Chambers

Date: 21 September 2018

[64] *Ibid* at 54.