MIRANDA GRANGE

CYBER WARFARE AND THE LAW OF ARMED CONFLICT

LAWS 533: LAW OF ARMED CONFLICT

RESEARCH PAPER

FACULTY OF LAW

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VICTORIA UNIVERSITY OF WELLINGTON

2014

Contents

Abstract

This paper discusses cyber warfare and its intersection with the law of armed conflict. Cyberspace creates a unique battlefield with many challenges. This paper tackles four of these challenges: distinguishing warfare acts from criminal activities; what amounts to an armed attack in cyberspace that justifies a State's right to self-defence; target distinction; and direct participation in cyber hostilities. It is the author's determination that the law of armed conflict does apply in cyberspace however two additional changes are needed for the traditional laws to have any practical effect. These two variations include the extension of the traditional criteria of armed attack to include severe data loss as tangible property damage; and re-examining the framework of direct participation.

Word length

The text of this paper (excluding abstract, table of contents, footnotes and bibliography) comprises approximately 7,684 words.

Introduction

Cyberspace has eliminated traditional geographic boundaries. States, organisations and individuals are today linked by vast, interconnected networks to disseminate information and data at a rapid rate. Everyday activities – from banking and sharing musings through blogs or email, to controlling systems and infrastructure – occur through digital networks in interconnected infrastructure.

Alongside the extensive utilisation and uptake of cyber operations, there arises a great risk that these linked systems and networks, and the data contained therein, may become the target of intentional malicious acts by States and non-State actors. It is not surprising that cyberspace has become a new frontier for attack given the ease and global uptake of cyber connectivity.

There is global concern that the nature and scope of cyber-attacks could cause far-reaching and devastating consequences. The concern of cyber warfare manifests in the law of armed conflict (LOAC) especially given the potential impact on civilian populations. This paper will canvas five selected issues in LOAC as applying to cyber warfare:

- **Chapter One:** Outlining four methods of cyber warfare and distinguishing criminal acts from acts of war;
- **Chapter Two:** The application of LOAC applies to the cyberspace jurisdiction and the principle of State attribution;
- **Chapter Three:** The application of *jus ad bellum* to cyberspace, including the prohibition on the use of force, self-defence, and armed attacks;
- **Chapter Four:** The problem of distinguishing targets in cyberspace; and
- **Chapter Five:** The difficulties with applying the traditional criteria of direct of direct participation to cyberspace hostilities.

I The methods of cyber warfare

The first step in this investigation between cyberspace and LOAC is to determine the parameters of a cyber-attack. In particular when does such an attack cross the boundary from a mere criminal act to an act of war. Given the uptake of cyber operations on a global scale, it is unsurprising that digital networks are prone to numerous attacks, for a variety of motives, by a number of actors. The benefits of using cyberspace also apply to those who wish to cause damage to such digital operations, focusing on speed and ease of access. These types of attacks create new challenges to information technology and data security professionals globally as well as to those who use such information, including civilian populations, governments and military personnel.

Cyberspace is more than what is known as the 'World Wide Web' (the 'Internet'); the Internet is the open part of a much larger virtual reality known as cyberspace.[1] Cyber-attacks occur when individuals or groups attack networks or data in cyberspace with the premeditated goal to destabilise or corrupt these digital systems. The reasons behind such attacks are as wide-reaching as the systems involved and may include creating an annoyance to the target, individual financial gain, espionage, or more sinister motivations. Cyber warfare occurs when malicious cyber-attacks escalate as military objectives on the international stage. Cyber-attacks which are used solely to collect information, including for espionage and spying purposes, are not enough to escalate such attacks into the realm of cyber warfare.[2]

A Cyber-attacks in the criminal jurisdiction

It is important at the outset to outline the difference between criminal acts and acts of war in cyberspace. Cyber-criminals normally steal data or disrupt networks

[1] Richard Clarke and Robert Knake *Cyber War: The Next Threat to National Security and what to do about it* (HarperCollins Publishers, New York, 2010) at 70.
[2] Michael Schmitt *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) at 192-193 [the 'Tallinn Manual'].

for financial gain.[3] The most common motives behind criminal cyber-attacks are to steal trade secrets, credit card details, identities, and intellectual property.[4] The biggest threat today to private organisations is reportedly cyber-crime from corporate spies or 'insider hackers'.[5] Most States regard it a criminal offence if an individual accesses information stored on a computer, or transmitted over a network, without authorisation or mandate.[6] Generally it is also a criminal offence to cause damage to data or systems through any type of cyber-attack. Obviously the strength and wording of such offences differ between territories.[7]

One of the important discussions in relation to acts of cyber warfare is the classification of espionage activities. Cyber-criminals can also undertake covert attacks for espionage reasons (foreign hackers accessing commercially sensitive information) or for 'hacktivism' (disrupting services to promote a cause).[8] In some cases cyber espionage does destabilise diplomacy and impacts on State sovereignty, but an action more than a criminal offence is required for cyber warfare.[9] Acts of cyber-crime, espionage and cyber warfare may look similar and can follow the same methods, which serves to illustrate that this analysis is a difficult one. When criminal actions escalate towards causing damage to persons, property or targets for military objectives, then such cyber-attacks enter the jurisdiction of LOAC. Such attacks are acts of cyber warfare. This exploration is one of threshold and may be difficult to determine given the methods are the same.[10]

---

[3] Dorothy Denning "Cyber Security as an Emergent Infrastructure" in Robert Latham (ed*.) Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (The New Press, New York, 2003) at 31; and New Zealand Government "New Zealand's Cyber Security Policy" (June 2011) Department of the Prime Minister and Cabinet <www.dpmc.govt.nz> at 5 [the 'NZ Cyber Security Policy].
[4] Denning, as above; and NZ Cyber Security Policy, at 3.
[5] Denning, as above.
[6] At 28.
[7] As above.
[8] Denning, as above, at 30; and NZ Cyber Security Policy at 5.
[9] Jeremy Rabkin and Ariel Rabkin *To Confront Cyber Threats, We must Rethink the Law of Armed Conflict* (Koret-Taube Task Force on National Security and Law, Hoover Institution, Stanford University, 2012), 11; and Yoram Dinstein "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference" (2013) 89 International Law Studies 276 at 284.
[10] Nathan Sales "Regulating Cyber-Security" (2013) 107 Northwestern University Law Review 1503 at 1523.

The line between espionage and warfare is so blurry that Russia is leading a small number of States who have called for an international arms treaty on cyber espionage.[11] These States wish to regulate the targeting and methods of cyber-attacks used for espionage. Unsurprisingly Richard Clarke, a former White House cyber-security official under three United States presidents, fervently disagrees with this idea and strongly argues that these kinds of cyber activities and operations are necessary for a State to protect itself from aggressors.[12] The activities are offensive to prepare adequate defences when faced with potentially deliberating attacks in war. Richard Clarke argues that:[13]

> An arms control agreement limiting cyber espionage is not clearly in our [the United States] interest, [as it] might be violated regularly by other nations [Russia], and would post significant compliance-enforcement problems.

With blurred lines in cyber warfare also with the application of State attribution (Section K), targeting (Chapter IV), and direct participation in hostilities (Chapter V), it may be time to look whether an international treaty clarifying these issues is required.[14] It is especially evident that cyber espionage by non-State actors may look and feel very similar to cyber warfare.[15] As discussed blow, this author disputes whether a convention is needed here and is wary whether such agreement would ever be reached in today's political climate.[16]

B Methods of cyber-attack

There are broadly four types of mechanisms that can be employed for cyber-attacks. These types of attacks generally occur on a sliding scale of severity with

[11] Clarke and Knake, above n 1, at 235-237; and Rabkin and Rabkin, above n 9, at 11.
[12] Clarke and Knake, as above, at 235-236.
[13] At 237.
[14] There is a Council of Europe treaty addressing cyber-crime activities, see Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004). This Convention does not discuss acts of cyber espionage or warfare.
[15] John Murphy "Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?" (2013) 89 International Law Studies 309 at 322-334.
[16] Dinstein, above n 9, at 286; Murphy, as above; Vijay Padmanabhan "Cyber Warriors and the *Jus in Bello*" (2013) 89 89 International Law Studies 288 at 307; and Jack Beard "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law" (2014) Vanderbilt Journal of Transitional Law 67 at 93.

many means of deployment in each category, and each method preceded by the previous step. It is noted that this list is the author's own based on her academic and technical research in this subject. These four steps are simplified for the purposes of brevity, intended to be non-exhaustive, and serve the purpose of outlining some of the common methods of cyber-attack using examples.

The four methods of cyber-attack are:

- Denying service or access to a network;
- Intercepting and redirecting traffic to capture information;
- Altering or destroying data on a network; and
- Taking undetected and complete control of computers and networks.

C Step One: Denying service or access to a network

This is the first step in a cyber-attack whereby attackers gain access to a network or computer and prevent straightforward access to users of the system. Such attack is common as it is at the minor end of the scale. A cyber-attack of this nature would include stopping (blocking) personal email traffic or access to a cloud-based storage account.[17] One widespread method of denying service or access to a network is by a 'distributed denial of service' (DDOS) attack.[18] DDOS attacks happen frequently for aggravation and criminal purposes.

DDOS attacks can be carried out is by using automated (ro)bots to access websites repeatedly on a network with such unusually high volumes that the attack causes the network to go offline (crash).[19] This tactic is used both in criminal attacks and in conflict situations. DDOS attacks of this nature were employed by Russia in 2007 in response to the Estonian government's decision to relocate a Soviet Union

[17] Before the rapid uptake of computers, this type of attack was referred to as a 'black fax attack' where targets were sent never-ending faxes intended to use up the recipient's toner, paper or ink. See Douglas Rushkoff "Extreme response not a solution" (17 July 2002) The Guardian <http://www.theguardian.com>.
[18] Clarke and Knake, above n 1, at 13-14; and Roxana Georgiana Radu "The Monopoly of Violence in the Cyber Space: Challenges of Cyber Security" in Enrico Fels, Jan-Frederik Kremer and Katharina Kronenburg (eds.) *Power in the 21st Century: International Security and International Political Economy in a Changing World* (Springer-Verlag Berlin Heidelberg, Germany, 2012) at 144.
[19] "Denial of Service Attacks" Incapsula <http://www.incapsula.com>.

World War II memorial. Russia allegedly launched prolonged DDOS attacks against government and national websites as well as online infrastructure.[20] In 2008, Russia again used this method against Georgia and followed these cyber-attacks by conventional armed fighting including dropping bombs.[21]

Clearly Russia is not the only State to utilise this kind of attack against another. China and the United States are also both suspected of being attackers and victims of DDOS attacks in the international sphere.[22] Members of an Iranian group, Izz ad-Din al-Qassam Cyber Fighters, are believed to have carried out DDOS attacks against American financial institutions in the past few years to protest the degrading personification of the Prophet Muhammad in the YouTube movie 'Innocence of Muslims'.[23]

D Step Two: Intercepting and redirecting traffic

This method of cyber-attack consists of intercepting and redirecting traffic to fake websites unbeknownst to users. The objective of these attacks is to capture the key used to encode information or to skim (steal) data from users. Such attacks are sometimes initiated by opening an email to a fake website, and are habitually caught by firewalls or antivirus software.[24] Another iteration of this type of cyber-attack is the introduction of malware into a computer or network which tracks users' inputs

[20] These attacks have been attributed to the Nashi Youth activist group with Russian government involvement. Clarke and Knake, above n 1, at 11-16; Radu, above n 18, at 138 and 145; Sales, above n 10, at 1504-1505; Michael Schmitt and Liis Vihul "Proxy Wars in Cyberspace: The Evolving International Law of Attribution" (2014) 1 Fletcher Security Review 55 at 55-56; and Ian Traynor "Russia accused of unleashing cyberwar to disable Estonia" (17 May 2007) The Guardian <http://www.theguardian.com>.

[21] Clarke and Knake, as above, at 18-20; Schmitt and Vihul, as above, at 55; and "Roundtable on Cyberwar and the Rule of Law" (15 October 2012) University of Pennsylvania Law School <www.law.upenn.edu> ['Roundtable'].

[22] Roundtable, as above; Leon Panetta "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (11 October 2012) United States Department of Defense <http://www.defense.gov>; Phil Muncaster "India to greenlight state-sponsored cyber attacks" (11 June 2012) The Register <http://www.theregister.co.uk>; and Pierluigi Paganini "Nation state sponsored attacks: the offensive of Governments in cyberspace" (12 November 2012) Security Affairs <http://securityaffairs.co>.

[23] Jennifer Bjorhus "Group halt bank cyberattacks" (29 January 2013) Star Tribune <http://www.startribune.com>; and Hollie McKay "'Innocence of Muslims' producer's identity in question; actors say they were duped, overdubbed" (13 September 2012) Fox News <http://www.foxnews.com>.

[24] Clarke and Knake, above n 1, at 14.

and feeds back information to attackers. Reportedly a third of such attacks involving interception or redirection are financial in nature, aimed at stealing individual bank passwords for monetary gain.[25]

This step has great traction in cyber-criminal acts but does not have much publicity in international conflicts as it often occurs alongside more devastating attacks in the next two steps.

E Step Three: Altering or destroying data

In this method of cyber-attack, hackers gain unauthorised access to networks with the intent to corrupt, alter or destroy data. The targets of this step can include private and/or government networks for both criminal and/or warfare motives. Such access can be gained through viruses and malware planted in a computer system; malware accesses the system (as outlined in step two), and computer viruses (or worms) adapt and/or delete data.

This type of cyber-attack is more than simply skimming information. Rather, it completely changes or adapts data to the detriment of the owner or user. Or, as occurred in the 2003 'Titan Rain' against the United States Department of Defense and NASA, data can be deleted forevermore.[26] As with the previous steps, these types of attacks occur in both the criminal and conflict jurisdictions.

Government and military databases have been targeted by this method of cyber-attack. Non-State key infrastructure organisations have also been embattled. Such attacks generally occur through the infection of malware via of user emails inside such networks. In August 2012 a computer virus called 'Shamoon' infected computers at Aramco, a private Saudi Arabian oil company.[27] This email-delivered virus caused crucial system files to be overwritten and more than 30,000 computers

[25] "Kaspersky Lab Study: about one third of all phishing attacks aimed at stealing money" (2 April 2014) Kaspersky Lab <http://www.kaspersky.com>.
[26] It has not been revealed how access was gained to these systems but terabytes of information was deleted and has not resurfaced. This attack is generally attributed to China. See Noam Lubell "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?" (2013) 89 International Law Studies 252 at 254; and Tom Espiner "Security experts lift lid on Chinese hack Attacks" (23 November 2005) zdnet.com <http://news.zdnet.com>.
[27] Panetta, above n 22.

were rendered useless and destroyed.[28] Within a week, there was a similar attack in Qatar on RasGas.[29] Both attacks have been attributed to Iran.[30]

Of higher global profile, a computer worm called 'Stuxnet' infiltrated the Natanz's nuclear plant network in Iran.[31] This malware was purportedly introduced into the network through a USB (universal serial bus) stick and had the effect of breaking centrifuges.[32] The result was that these parts – which separate the uranium particulates in the nuclear enrichment process – were required to be replaced more often than normal. Stuxnet lay undetected in the plant's systems for at least three years. This attack has been attributed to Israel and the United States, with major media outlets claiming that this was the first time that "the United States used computer programs for purposes that until recently could only be achieved through bombs and other conventional weapons."[33] This type of attack unmistakably occurs in the cyber-criminal jurisdiction as well as in cyber conflicts. A similar cyber-attack to Stuxnet was reported in Illinois in 2012 where criminal attackers caused a water pump to burn out by turning the pump on and off repeatedly.[34]

This method of cyber-attack has importance in any discussion involving LOAC as it identifies that cyber-attacks may not result in physical property harm but have other, perhaps more far-reaching, consequences (see Sections N and O). Such outcomes include economic and financial suffering, data loss and network intrusion.

---

[28] Shamoon performed a piece of self-executing code (a wiper) which replaced crucial systems files with an image of a burning flag of the United States, as well as overwriting databases. See Panetta, as above.
[29] As above.
[30] Schmitt and Vihul, above n 20, at 55; and Christopher Bronk "The Cyber Attack on Saudi Aramco" (1 April 2013) Survival: Global Politics and Strategy <http://www.iiss.org>.
[31] Stuxnet was supported by a data-mining virus (Flame) and a reconnaissance virus (Dugu). See "Humanity in the Midst of War: Blog related to the laws of armed conflict (LOAC)" (2 October 2012) lawsofarmedconflict.com <http://lawsofarmedconflict.com> ['LOAC blog'].
[32] Nate Anderson "Confirmed: US and Israel created Stuxnet, lost control of it" (1 June 2012) Arstechnica <http://arstechnica.com>.
[33] As above; Roundtable, above n 21; Murphy, above n 15, at 314; and Ruth Levush "The New Cyber Battlefield: Implications under International Law of Armed Conflict" (10 October 2012) Law Librarians of Congress <http://blogs.loc.gov>.
[34] "International cyber strike attacks US infrastructure" (19 November 2011) The New Zealand Herald <http://www.nzherald.co.nz>.

F Step Four: Full control of computers and networks

The ultimate goal of those engaged in cyber-attacks in both the criminal and warfare areas is not only to steal, adapt or destroy data, but principally to gain full control of computers and networks in cyberspace and to lock out the user's administration from their own network. As an extreme manifestation of occupation in the digital sphere, this is the specific end-goal of those involved in cyber warfare. Such methods would use the earlier described methods, culminating in this vicious consequence. This type of colossal access has not been reported in any international conflict but is a constant fear for cyber security specialists.[35]

G Defending cyber-attacks

Due to the significant amount of damage that can occur as a result of such cyber-attacks there is universal concern regarding the prevention and defence of such attacks. Concern is evident at both the cyber-criminal level and at the wider implication of cyber warfare.

Many States have set up cyber-security governmental organisations to protect against the threat of cyber-attacks. In 2007, McAfee, a global security firm, estimated that 120 countries had already developed ways to use the internet to target financial markets, government computer systems, and utilities.[36] The United States has been particular vocal about their efforts in this jurisdiction. In 2008, after a cyber-espionage attempt aimed at its secret military network (SIPRNET),[37] the United States Cyber Command was established and henceforward has a role in developing cyberwar capabilities. The Pentagon also maintains the 'Defense Advanced Research Projects Agency' (DARPA), which has recently funded Plan X, having the goal of protecting computer systems as well as developing cyber warfare capabilities to disrupt or destroy enemy system. In June 2009 the United Kingdom launched their

[35] Warwick Ashford "Lock up admin accounts to defeat hackers, says Cyber-Ark" (19 June 2013) ComputerWeekly <www.computerweekly.com>.
[36] Roundtable, above n 21; and Paganini, above n 22.
[37] Roundtable, as above; Paganini, as above; Schmitt and Vihul, above n 20, at 55; Clarke and Knake, above n 1, at 34-44; and Paul Walker "Organizing for Cyberspace Operations: Selected Issues" (2013) 89 International Law Studies 341 at 341-342.

national cyber security plan[38] and New Zealand followed suit in June 2011.[39] It is also predictable that North Korea, Russia, Iran, Iraq, India and China boast of advanced cyber warfare capabilities.[40]

II The application of the law of armed conflict in cyberspace

H Cyberspace as a battlefield

Cyberspace creates a unique battlefield in LOAC. Cyberspace guarantees that individuals and groups involved in cyber-attacks can be coordinated in an extremely timely manner; that attacks on targets can be delivered accurately; that target or attack information can be shared fast; and that decisions can be made much more rapidly than ever before in history.[41] These attributes exist however inaccurate or correct the sources of information may be. States and individuals that traditionally could not compete on the conventional combat zone, or could not defend against larger States with more resources, find themselves on a virtual battlefield using computer code as weapons.[42]

The scope of targets that may be subjected to cyber-attacks is essentially unlimited and could have vast implications for civilian populations due to the dual purpose of most key infrastructure items.[43] The principle of distinction in cyberspace is discussed in more detail in Chapter IV. Taken literally, anything connected in cyberspace could be a target – such as corrupting financial data, destabilising key utility infrastructure, grounding an airline, or causing a satellite to spin out of orbit.[44] This universality highlights that there is a current, real risk if

[38] Radu, above n 18, at 146.
[39] NZ Cyber Security Policy, above n 3.
[40] Panetta, above n 22; Roundtable, above n 21; Muncaster, above n 22; and Denning, above n 3, at 31.
[41] James Adkisson and others *Law of Armed Conflict: Implications for Navy Cyber Strategy* (Masters of Information Technology Strategy Practicum – 2012, Carnegie Mellon University, Pittsburgh, Pennsylvania, 3 August 2012) at iii and 1.
[42] At 1.
[43] Emphasis added. Eric Mifflin "The Law of Armed Conflict in the 21st Century: A Critical Examination of the Legal Relationship between State and Non-State Entities" (Master of Arts in Political Science thesis, University of South Dakota, United States, 2010) at 41-42.
[44] Clarke and Knake, above n 1, at 70.

cyber-attacks are carried out correctly, accurately, with an eye for war. If so, then "cyber weapons can be as devastating as conventional munitions"[45] and may cause considerable collateral damage, including civilian casualties.

In 2012 the previous United States Secretary of Defense, Leon Panetta, spoke about the brutality that could occur in cyber warfare and warned executives to be mindful that this is a very real risk:[46]

> [The Internet] is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. … A cyber attack perpetrated by nation states and violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

I Application of LOAC

The modern wave of rules prohibiting extreme brutalities in times of war can be traced back to the end of World War II when the international community agreed to regulate the use of force to prevent such atrocities from reoccurring. New methods of war, including cyber-attacks, were not within the realm of common contemplation when formulating these principles. Thus there are some obvious divergences between traditional rules and new methods of war. Cyberspace creates new challenges in LOAC given its interconnectivity and the spread of use for global operations.[47]

Do these existing laws apply as is without modification or is some modification required? This was the debate in the international legal community during the 1990s and early 2000s. One of the preliminary arguments focused on whether cyber warfare and its weapons should be banned in the same way as biological or chemical weapons. This argument has settled now with States and scholars in agreement that cyber operations will continue to grow and thus cyber warfare is an allowable method of war. The balance of a State's interest in maintaining global

[45] Adkisson and others, above n 41, at 4.
[46] Panetta, above n 22.
[47] Kenneth Watkin "The Cyber Road Ahead: Merging Lanes and Legal Challenges" (2013) 89 International Law Studies 472 at 474.

consensus against using cyber weapons is overruled by the global interest in favour of such weapons.[48] Richard Clarke states this discussion is settled as it is impossible to justify that cyber-attacks cause undue harm equivalent to gas strikes or expanding bullets.[49] For him "[t]he focus [should] be on keeping cyber-attacks from starting wars, not on limiting their use once a conflict has started".[50]

There are of course less restrictive approaches to banning cyber weapons and that is where LOAC comes into play. The current discourse in international law focuses on what laws apply to cyberspace and whether traditional rules should be developed to take into account this unique battlefield.

J The Tallinn Manual

Following the attacks on Estonia in 2007, the North Atlantic Treaty Organization (NATO) became interested in the significance of global cyber warfare. A NATO Centre was set up in Tallinn, Estonia. This location was deliberate as this was the site of arguably the first case of international cyber warfare which occurred in protest to the removal of the Bronze Soldier statue.[51] Some commentators have called this attack 'Web War I' and refer to Estonia as 'E-stonia' given its dependence on cyberspace.[52] By 2007, 98% of all Estonian bank transactions were done electronically and over 80% of tax declarations were done online.[53] At the time Estonia was one of the most wired nations in the world, ahead of the United States, and only outdone by South Korea.[54] The Russian attacks weakened the already divided nation and thus NATO was forced to take notice.

The NATO Cooperative Cyber Defence Centre of Excellence was established and initiated a process that led to the preparation of guidelines to address LOAC as

[48] Clarke and Knake, above n 1, at 239.
[49] At 239-240.
[50] At 240.
[51] Radu, above n 18, at 138; and Traynor, above n 20.
[52] Sales, above n 10, at 1504-1505; and Matthew Waxman "Cyber Attacks as "Force" under UN Charter Article 2(4)" (2011) 87 International Law Studies 43 at 45.
[53] Radu, above n 18, at 145.
[54] Clarke and Knake, above n 1, at 13; and Sales, above n 10, at 1504.

applicable to cyberspace.[55] The outcome of this initiative was almost universal agreement among experts that the existing LOAC applies to cyber space.[56] The process was led by Professor Michael Schmitt of the United States Naval War College – an extensive writer on this subject – and took four years, involved 20 experts, culminating in the results being published in 2013 (the Manual).[57]

It is recognised that the Manual must be approached and applied with care given it is non-binding and only selected experts from the field of cyber security participated. A wide breadth of experts were consulted in their personal capacity including lawyers, academics and technical experts.[58] The Manual is a useful first step towards clarifying the international law pertaining to cyber-attacks.[59] The International Committee of the Red Cross (ICRC) has also expressed its favour for the Manual and representations also observed the discussions leading up the Manual's finalisation.[60]

The present problem in this area of law is the interpretation of such laws as they apply to cyberspace. This interpretation question is stated as the principal reason why some States, such as Russia and China, publically disagree with the published Manual.[61]

K Principle of attribution

The attribution to States of the actions of non-State actors under LOAC is a problem in cyberspace. Rule 6 of the Manual applies this customary principle of

[55] Bill Boothby "UK Armed Forces Personnel and the Legal Framework for Future Operations: Further written evidence from Air Commodore (Retd) Bill Boothy, Doktor Iuris, former Deputy Director of Legal Services (RAF)" (December 2013) United Kingdom Parliament <www.publications.parliament.uk>.
[56] Tallinn Manual, above n 2, at 5; and Robin Geiss "Cyber Warfare: Implications for Non-international Armed Conflicts" (2013) 89 International Law Studies 627 at 631.
[57] See generally Tallinn Manual, as above.
[58] At 9 and 11; and Levush, above n 33.
[59] Tallinn Manual, above n 2, at 11; Schmitt and Vihul, above n 20; Boothby, above n 55; and David Wallace and Shane Reeves "The Law of Armed Conflict's 'Wicked' Problem: *Levee en Masse* in Cyber Warfare" (2013) 89 International Law Studies 646 at 649.
[60] "The law of war imposes limits on cyber attacks too" (1 July 2013) International Committee of the Red Cross <www.icrc.org>; and "What limits does the law or war impose on cyber attacks?" (28 June 2013) International Committee of the Red Cross <www.icrc.org>.
[61] Boothby, above n 55.

attribution to cyberspace and thus it follows that a State is responsible for non-State actors for cyber-attacks if they have effective or overall control over such actors.[62] This is a scale test and requires specific examination of the facts surrounding the conflict to determine the scope of a State's control. It remains clear that a State's intelligence agency personnel are classified as military personnel in cyber warfare acts and thus such actions of personnel are attributable to the State which they act on behalf of.[63]

L The actions of non-State actors

The scope and amount of control by the State is important for the principle of attribution. Commentary 11 to Rule 6 states that "[t]he State needs to have issued specific instructions or directed or controlled a particular operation to engage State responsibility."[64] Individuals or groups acting on their own volition will consequently not be attributed to a State and thus will not fall foul of the prohibition on use of force, though such individuals or groups may violate other laws.[65] The principle of attribution is met if a State provides insurgent hackers of another State tools to fight against their own State. Such a violation may constitute a contravention of LOAC similar to guerrilla warfare tactics in traditional battle.[66]

When finalising the Manual, the experts also comment that more support is needed than simply providing funds or express encouragement; effective or overall control would entail planning and supervision of State military objectives.[67] This control would be enough to attribute the acts of non-State recruits to a particular State, and thus that State would be accountable under the rules of armed conflict.

There is consensus in scholarship that sophisticated cyber-attacks, including Stuxnet, must be attributed to a State due to their complexity and sophistication.[68]

---

[62] Tallinn Manual, above n 2, at 29 and 32.
[63] At 43.
[64] At 33.
[65] At 44; Schmitt and Vihul, above n 20 at 62-63; and Michael Schmitt "Classification of Cyber Conflict" (2013) 89 International Law Studies 233 at 246.
[66] Tallinn Manual, above n 2, at 33-34 and 46.
[67] At 33; and Schmitt and Vihul, above n 20, at 64.
[68] Geiss, above n 56, at 630.

There is no conceivable situation where these types of attacks would have escaped the notice of a State or a coalition of States due to their exact targeting of objectives for a military purpose.[69]

III Jus ad bellum *and cyber-attacks*

Under *jus ad bellum*, cross-border military operations are not permitted due to the inter-State prohibition on the use of force by Article 2(4) of the United Nations Charter.[70] Taken alongside the rules contained in the Geneva Conventions and in customary international law, this ban on force is one of the cornerstones of international law.[71] States are bound by this prohibition either by ratification of the international treaty or by customary international law.[72]

The term 'use of force' in the Charter is not defined (which is not unusual given the international nature of the Charter)[73] but it is accepted that the use of force must require an armed attack[74] without regard to the type of weapons used.[75] Rules 10 and 11 of the Manual state that the use or threat of force prohibition extends to cyber operations.[76] Thus if a cyber-attack does meet the threshold of a use of force, aggressors would need to comply with the four main *jus in bello* principles under

[69] As above.
[70] Charter of the United Nations (1945), art 2(4). See also Paul Ducheine, Frans Osinga and Joseph Soeters (eds.) *Cyber Warfare: Critical Perspectives* (NL ARMS: Netherlands Annual Review of Military Studies 2012) at 116.
[71] See Charter of the United Nations, as above; Geneva Conventions 75 UNTS 31 (signed 12 August 1949, entered into force 21 October 1950); Protocol I Additional to the Geneva Conventions 1125 UNTS 3 (signed 8 June 1977, entered into force 7 December 1978); Protocol II Additional to the Geneva Conventions 1125 UNTS 3 (signed 8 June 1977, entered into force 7 December 1978); and Protocol III Additional to the Geneva Conventions 2404 UNTS 1 (signed 8 December 2005, entered into force 14 January 2007).
[72] Non-Member States are bound by customary international law. See Tallinn Manual, above n 2, at 43.
[73] At 45-46; and Adkisson and others, above n 41, at 6. Other key terms used in the Charter are also not defined, including "aggression" which lead to the General Assembly passing Resolution 3314 containing a Definition of Aggression as an annex. See *Resolution on the Definition of Aggression* GA Res 3314, XXIX (1974), Annex art 1.
[74] States facing an armed attack that does not constitute a use of force does not violate Article 2(4) of the Charter. See Tallinn Manual, above n 2, at 52; Ducheine, Osinga and Soeters, above n 70, at 116. See also the commentary on the *Nicaragua* judgment discussed in Tallinn Manual, above n 2, at 45.
[75] Tallinn Manual, as above, at 42.
[76] At 42-45.

LOAC. Cyber warfare would need to be undertaken for a defensible military reason (including to weaken an enemy); attack only military objectives; have an advantage that outweighs collateral harm; and does not cause unnecessary harm to the target.[77] It is important to remember that if a cyber-attack does not meet the threshold of using force, then such actions avoid international humanitarian law[78] and would only be punishable under a State's domestic legal system.[79]

A State can respond in self-defence if it is the target of illegal force by virtue of Article 51 of the Charter and Rule 13 of the Manual.[80] The right to self-defence can only be deployed if a State is responding to an armed attack or when a State is authorised to act under a Security Council resolution.[81] For the right of self-defence to be triggered as a violation on the use of force, an attack must be 'armed' which is interpreted narrowly and requires serious consequences.[82] If the use of force does not meet the threshold of an armed attack, the attacked State cannot resort to self-defence, though they can bring the matter before the Security Council, carry out non-forcibly counter measures, or perhaps sue (if jurisdiction exists).[83] The United States argue a narrower interpretation of the Charter and affirm that there is no gap between a use of force and an armed attack.[84] This view is the minority internationally.

It is also arguable whether the right of self-defence applies against non-State actors or only attacking States. Professor Schmitt believes that such actions are attributable to the State and therefore self-defence is appropriate in armed

[77] LOAC blog, above n 31.
[78] As above.
[79] For example, the Police and Justice Act 2006 (United Kingdom) which outlaws DDOS attacks and §1030 of the Computer Fraud and Abuse Act (United States) which makes DDOS attacks a federal crime.
[80] Tallinn Manual, above n 2, at 54; Adkisson and others, above n 41, at 9; and Laurie Blank "International Law and Cyber Threats from Non-State Actors" (2013) 89 International Law Studies 406 at 412.
[81] Rabkin and Rabkin, above n 9, at 3.
[82] Murphy, above n 15, at 316; Schmitt and Vihul, above n 20, at 67; and Blank, above n 80, at 412-413.
[83] Dinstein, above n 9, at 278.
[84] Schmitt and Vihul, above n 20, at 68.

attacks,[85] and there is nothing in Article 51 ensure that the right of self-defence only applies between States.[86] A State's right to self-defence in armed attacks applies then when acts of non-State actors are attributed to a State as discussed in Section K.

Given the prominence of United States, Russia and China in cyber warfare considerations, it is problematic to imagine a situation where a Security Council resolution for retaliation against a cyber-attack will remain un-vetoed by one of these States.[87] Thus the only way in practice that a State can use force in self-defence is if the cyber-attack meets the threshold of an armed attack. The question of when a cyber-attack transgresses from a criminal activity to an illegal use of force as an attack is an important one.[88]

M Armed attack

If a cyber-attack meets the threshold of an armed attack then LOAC automatically applies and retaliation in self-defence is an option to an invaded State.[89] If an attack does not meet the required threshold then the affected State would only be entitled to use force against the attackers otherwise they themselves may breach the prohibition on using force.[90]

It is important to note that none of the case studies provided in this paper have reached the threshold of an armed attack on their own – in the opinion of the Manual, international organisations and other experts – as the scale and effects of each cyber-attack were not enough objectively.[91] The cyber-attacks between Russia and Georgia in 2008 were covered by LOAC as they were part of an existing international armed conflict.[92]

[85] At 69-70.
[86] Blank, above n 80, at 413.
[87] Rabkin and Rabkin, above n 9, at 4.
[88] Dinstein, above n 9, at 278.
[89] Tallinn Manual, above n 2, at 47 and 55; Ducheine, Osinga and Soeters, above n 70, at 118 and 121; and Lubell, above n 26, at 258.
[90] Schmitt and Vihul, above n 20, at 60 and 62.
[91] Tallinn Manual, above n 2, at 57-58; and Geiss, above n 56, at 630 and 633.
[92] Tallinn Manual, as above, at 57-58 and 75-76.

In a traditional conflict, actions are judged by their effect or result, not on the extent of force used.[93] Kinetic attacks are considered an armed attack if they directly cause injury, death, or damage to property[94] and transcend borders.[95] The Manual is clear that a violation on the use of force also occurs if a cyber-attack causes personal or property damage, and such damage violates a State's sovereignty.[96] Under this traditional framework, if a cyber-attack takes complete control of a State's key network, and that control caused injury, death or damage to property, then this act would constitute an armed attack as a use of force that triggers the attacked State's right to self-defence per Article 51. If physical damage occurs on a scale large enough to violate State sovereignty, and physical replacements are required as a result of a cyber-attack, then there has been an armed attack that constitutes an illegal use of force.[97]

N Traditional framework of an armed attack

This threshold analysis generated animated debates by the experts creating the Manual. Some experts resolutely believed that the Stuxnet cyber-attack met the threshold of an armed attack as there was damage to property.[98] As mentioned previously in this paper, there have been no reported cyber-attacks that have reached the threshold of an armed attack under traditional LOAC. It is certainly evident that some attacks, such as Stuxnet and Shamoon, caused damage to physical property but it has not been determined whether this damage amounted to the violation on a State's sovereignty. The end result is that the Manual is silent on whether future attacks of this nature will meet the threshold of an armed attack. This investigation will accordingly occur on a case-by-case basis having regards to all the facts of the particular conflict.

[93] Ducheine, Osinga and Soeters, above n 70, at 116; and Schmitt and Vihul, above n 20, at 59.
[94] Ducheine, Osinga and Soeters, as above; and Sales, above n 10, at 1522.
[95] Tallinn Manual, above n 2, at 54.
[96] At 48, 55-57 and 106-109; Schmitt and Vihul, above n 20, at 59-60; Ducheine, Osinga and Soeters, above n 70, at 116; and Lubell, above n 26, at 264.
[97] Lubell, as above, at 265.
[98] Tallinn Manual, above n 2, at 58; and Murphy, above n 15, at 313-314.

There are some obvious acts that will not meet this high threshold of an armed attack. The Manual is clear that cyber-attacks with the intention to undermine confidence in a government will not constitute a use of force.[99] Neither will cyber-attacks that involve minor interruptions of non-essential services[100] or acts of cyber intelligence or espionage (discussed in Section A).[101] Most scholars agree that it is unlikely that blocking email access would be enough to meet the threshold,[102] regardless of how frustrating or aggravating this action may be to the population. These situations are consistent with international consensus that an event must be significant in order for LOAC to be incited, and more severe for a right of retaliation by force.

O The expansion of the traditional framework

The strict application of the traditional criterion may give some odd results in cyberspace which cannot be ignored, particular the focus on physical harm. It is the author's view that LOAC should acknowledge that there are types of cyber-attacks that may meet the threshold of the necessary violence of an armed attack without damage to persons or property.[103] In particular, the traditional framework needs to be expanded to take into account severe data loss as tangible property damage. Such an examination in LOAC is appropriate given the scale and effect that large data loss could have on a State and its population as a result of a cyber-attack. Such incidents could be crippling – for example, wide scale personal data obliteration (such as the deletion of personal banking or health records) or causing a major stock exchange crash.[104] Under the traditional criteria, if cyber-attacks cripple a network then the threshold of an armed attack would not be met unless the physical hardware needed

[99] Tallinn Manual as above, at 46.
[100] At 55.
[101] As above.
[102] See generally the discussion on Egypt's decision to turn off internet access within its borders in January 2011 during a period of civil unrest: Cassondra Mix "Internet Communication Blackout: Attack Under Non-International Armed Conflict?" (2014) 3 Journal of Law and Cyber Warfare 70; and Lubell, above n 26, at 265.
[103] Ducheine, Osinga and Soeters, above n 70, at 121 and 122.
[104] Tallinn Manual, above n 2, at 56.

to be replaced.[105] If a computer system was manipulated to shut down a State's electricity distribution network, this would also not reach the threshold of harm required under the traditional model as no physical destruction has occurred.[106] This focus on the damage to the tangible property, but not on the data itself, is absurd in cyberspace.

Regardless of this illogicality, there is no current consensus on a threshold of action that would permit self-defence outside of the traditional criteria. States and scholars are divided on this point.[107] Conservative scholars argue that if a cyber-attack does not meet the traditional criterion, then it will not qualify as a use of force and thus retaliation under self-defence would not be appropriate.[108] While negotiating the Manual, there were heated deliberations between experts on whether the first three types of attacks discussed in this paper (denying access to a network; capturing information; and altering or destroying data) should meet the traditional threshold. Liberal experts, to whom this author is sympathetic, argue that placing malware or deleting/altering data should meet the threshold of an armed attack due to the level of harm that could be caused.[109] The Manual leaves this question open for the time being.

Current jurisprudence is emerging that battles in cyberspace should focus the level of harm caused rather than the violence or type of the attack, as in traditional battles.[110] Rules 11 and 13 of the Manual simply state that an armed attack that constitutes a use of force in cyberspace will depend on the scale and effect.[111] The Manual's silence on types of events outside the traditional framework indicates that such examination would need to happen on a case-by-case basis having regard to the conflict.

---

[105] Lubell, above n 26, at 266.
[106] Geiss, above n 56, at 644.
[107] See Tallinn Manual, above n 2, at 56.
[108] Schmitt and Vihul, above n 20, at 59; Adkisson and others, above n 41 at 8; and Eric Talbot Jensen "Cyber Attacks: Proportionality and Precautions in Attack" (2013) 89 International Law Studies 198 at 201.
[109] Schmitt and Vihul, as above, at 60.
[110] Lubell, above n 26, at 265.
[111] Tallinn Manual, above n 2, at 45 and 54.

Another argument in this sphere is whether the traditional definition should be widened in cyberspace to include financial loss. Experts of the Manual were divided on whether financial loss would meet the scale and effect threshold.[112] It is the author's view that while financial and economic hardship is easy to think about in cyberspace operations[113] (especially given the dependence on online banking and tax declarations, as examples) this discussion strays LOAC too close to the jurisdiction of cyber-crime. LOAC is not suitable to be used for acts of criminality and cyber espionage[114] The Manual is silent on these situations as well, so a factual will analysis will need to occur.

IV The principle of distinction in cyberspace

The *jus in bello* principle of distinction creates rules around targets that can and cannot be attacked in warfare situations. Article 48 of Additional Protocol I to the Geneva Conventions states that "[t]he Parties to the conflict shall at all times … direct their operations only against military objectives".[115] Rule 31 of the Manual applies this principle of distinction to cyber-attacks.[116] The Manual acknowledges this extension of the customary law notion that where cyber-attacks are directed at military targets for legitimate objectives, and precautions have been taken to prevent disproportionate collateral attacks then they operate within the legal realm of LOAC, so long as they are not deceitful.[117] If a cyber-attack targets civilians, or which is by nature indiscriminate,[118] then such attack may breach Rules 32 and 37 of the Manual and contravene of LOAC.[119]

[112] At 56.
[113] Rabkin and Rabkin, above n 9, at 7.
[114] Watkin, above n 47, at 492; and Beard, above n 16, at 127-128.
[115] Protocol I Additional to the Geneva Conventions, above n 71, at art 48; Boothby, above n 55; Ducheine, Osinga and Soeters, above n 70, at 122; and Lubell, above n 26, at 253.
[116] Tallinn Manual, above, n 2, at 110.
[117] At 113-124; and Louise Doswalk-Beck "Confronting Complexity and New Technologies: A Need to Return to First Principles of International Law" (2012) 106 American Society of International Law 107 at 107-108.
[118] Tallinn Manual, as above, at 156; and Doswalk-Beck, as above, at 108.
[119] Tallinn Manual, as above, at 113 and 124-125.

It is important to remember that a cyber-attack must be an 'attack' against a civilian target to be prohibited under this principle; transmitting email messages to civilian populations is not enough to violate this standard as this would not meet the threshold of an attack.[120] This point links in with the discussion in Section M.

P Interconnectivity of cyberspace

The principle of distinction in cyberspace is difficult given the interconnectivity of networks and computers. Such interconnectivity does not rely on the habitual split between civilian and military purposes.[121] The ICRC also acknowledges this struggle of distinction.[122] Developed countries are particularly reliant on cyber operations for essential services to serve both military and civilian populations – such as water, electricity, communications and transportation.[123] It is difficult to differentiate military and civilian uses for these services due to their dual use character. Targets of cyber-attacks are thus likely to mirror this dual purpose.[124]

Because of this inherent double purpose, most developed countries insist that their primary infrastructure is 'double coded'.[125] Applied historically, city and castle walls were double coded for defence and economic reasons. Today the same idea exists for cyberspace: access to military infrastructure is restricted and maintenance kept separate from the public mainstream. Yet military targets are still reliant on public roads and communication pipelines.

Q Dual use objects

Rule 39 of the Manual positions that dual use objects are deemed military objectives.[126] Dual statuses cannot co-exist and thus, if any use is military, then it is

[120] At 112-113.
[121] Lubell, above n 26, at 253; and International Committee of the Red Cross, above n 60.
[122] "Weapons: ICRC statement to the United Nations" (16 October 2013) International Committee of the Red Cross <www.icrc.org>.
[123] Robert Latham (ed.) *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (The New Press, New York, 2003) at 14.
[124] Ducheine, Osinga and Soeters, above n 70, at 122; and Sales, above n 10, at 1524.
[125] Latham, above n 123, at 15.
[126] Tallinn Manual, above n 2, at 134.

deemed a military object and can be targeted.[127] This rule means practically that telecommunications and electricity networks for most countries, including New Zealand, would be deemed military objectives. Such dual use targets may also include power plants, satellites, or air traffic control towers.[128]

This rule may seem extreme initially, given the interconnectivity of cyberspace and that military uses may be indistinguishable from civilian uses. Civilian items could easily become targets given the vast number of digital networks or infrastructure that is used by military and civilians alike. The Manual also provides this troubling statement:[129]

> Although an attacker may not know with certainty which roads will be travelled by enemy military forces (or which road will be taken if another is blocked), so long as it is reasonably likely that a road in the network may be used, the network is a military objective subject to attack.

However, despite initial alarm, it is important to remember that there are some qualifications here. The dual use rule is subject to the principle of proportionality; cyber operations must reach the threshold of an armed attack; and only targets used for military purposes (if discernible) can be attacked.[130] These qualifications provide some comfort at least to the author, though relief could be limited in practice.

R Impracticalities of distinction

As a result of interconnectivity, there have been calls from a minority of scholars to ban cyber warfare tactics on financial institutions.[131] This argument stems from the fact that most individuals and every State (except, arguably, North Korea)[132] have a stake in the reliability of global banking infrastructure. Thus

[127] As above.
[128] Walker, above n 37, at 353.
[129] Tallinn Manual, above n 2, at 135.
[130] As above.
[131] Clarke and Knake, above n 1, at 245-246; Watkin, above n 47, at 496; and Beard, above n 16, at 127-128.
[132] Clarke and Knake, as above, at 246; and Watkin, as above, at 496-497.

launching an attack against this type of target would be counter-intuitive.[133] Such an attack on a financial institution could have wide-reaching effects causing the undermining of markets and confidence internationally.[134] The author disagrees with this argument. This idea is inherently Western in that it places large importance on commerce.[135] This debates shifts the goalpost of LOAC uncomfortably close to cyber espionage and cyber-crime. This is not the role of LOAC.

There is also wider current debate internationally about whether the principle of distinction should exist at all in cyberspace due to the practicalities of interconnectivity.[136] As an example, 98% of the United States federal government communications traffic is transported through civilian networks,[137] illustrating that it is difficult, or impossible, to separate targets. Just as there is no current consensus on the threshold as to what constitutes an armed attack in cyberspace, there is also no consensus on what type of cyber-attack against civilian cyber operations would meet the threshold sufficient for a State to retaliate in self-defence. Again this will need to be examined on a case-by-case basis having regard to the effects outlined in Section M and this debate will continue.[138] To date, there has been no international treaty proposed to clarify the principle of proportionality in cyberspace and the author recognises that any agreement to waive this fundamental *jus in bello* principle is highly doubtful.

V Direct participation in cyber warfare

Another important question for LOAC is how to identify civilians whom are directly participating in hostilities in cyberspace. Once they meet this divide, they

[133] Clarke and Knake, as above.
[134] As above.
[135] Beard, above n 16, at 128.
[136] Lubell, above n 26, at 253.
[137] Sales, above n 10, at 1524.
[138] Adkisson and others, above n 41, at 8.

can become targets of attacks under international law.[139] As in traditional conflicts, if a civilian directly participates in cyber hostilities then they lose certain civilian privileges.[140] Arguably, it may be unlikely that those involved in cyber warfare acts will be captured by enemies or want to invoke protections under prisoner of war status, unlike those in traditional warfare.[141] One of these reasons is because, unlike conventional methods of war, one of the goals of cyber warfare activities is to remain anonymous through computer infrastructure, achieved through means such as masking your internet protocols (IP) address.[142] This is easy to do for the short term; this is achievable for the time period required to execute cyber-attacks.[143] There is an immense problem in immediately identifying natural persons behind a keyboard in order to respond to such attacks and attackers in a timely manner. Identifying IP addresses and pinpointing where attacks originate is time consuming and involves technical forensic analysis.[144]

S Traditional participation in warfare

Determining direct participation of those in cyber warfare is complex as there are numerous parts to a single cyber-attack and there are many methods of attacks that may come together to create a cyberwar. Participants may also not look like participants of those involved in traditional conflicts. The skills deployed in criminal cyber-attacks look the same as those held by trained information technology professions, not just abilities gained by usual military training.[145]

---

[139] Protocol I Additional to the Geneva Conventions, above n 71, art 51(3); Protocol II Additional to the Geneva Conventions, above n 71, art 13(3); Tallinn Manual, above n 2, at 95 and 115-118; International Committee of the Red Cross, above n 60; and Emily Crawford *Virtual Battlegrounds: Direct Participation in Cyber Warfare* (Legal Studies Research Paper No. 12/10, Sydney Law School, The University of Sydney, February 2012) at 3-4.
[140] Tallinn Manual, as above, at 95 and 104.
[141] Rabkin and Rabkin, above n 9, at 11.
[142] Padmanabhan, above n 16, at 295.
[143] There is an additional issue here relating to the time period that civilians are deemed to directly participate in hostilities. In cyber-attacks, does this simply mean while they are executing a code sitting in front of a computer? See Padmanabhan, as above, at 300-301.
[144] Geiss, above n 56, at 636; Dinstein, above n 9, at 282; and Waxman, above n 52, at 50.
[145] Rabkin and Rabkin, above n 9, at 9.

Cyberspace operations may not have the same degree of organisation as those in traditional warfare situations.[146] If they do not meet these thresholds, then there is no action under LOAC. Organised groups in cyberspace are not likely to conform to the traditional conditions of groups, such as having a commander, the wearing of distinctive emblems or the open carrying of arms.[147] It is doubtful that groups participating in cyber-attacks of a warfare nature will all wear physically uniform identifiers nor will they carry discernible weapons (either laptops or guns), though they may have individuals who issue commands or directives. Members of a combatant group in cyberspace may not know, or even be able to identify, their commander and they certainly are unlikely to be subject to an internal disciplinary process to ensure compliance with group rules.[148] There is also current debate on whether groups that are organized solely online over various locations, would meet the required threshold of organization for its civilian attacks to directly participate in hostilities.[149] They have no physical headquarters or meeting place, and are unlikely to meet the traditional threshold.[150]

There was also dissention on this point in the Manual discussions particularly concerning the requirement of uniforms. Some experts believed that an international treaty needs to be created to ensure that the requirement to wear a uniform or emblems is expressly waived in cyberspace.[151] The author has some sympathy for this given this requirement will be unlikely to exist for groups collected in cyberspace spanning geographies. Other Manual experts argued that this requirement was absolutely necessary under customary international law.[152] This remains unsettled and no such treaty has eventuated.

[146] Geiss, above n 56, at 634-635.
[147] Tallinn Manual, above n 2, at 97; Padmanabhan, above n 16, at 485
[148] Tallinn Manual, as above, at 98; and Schmitt, above n 65, at 247.
[149] Geiss, above n 56, at 636.
[150] As above.
[151] Tallinn Manual, above n 2, at 99.
[152] At 99-100.

T Examples of direct participation in cyberspace

It is clear than employees of military, or contractors of intelligence and military organisations will be directly participating in cyber war.[153] This includes if they are engaged to simply write malicious code or executed given code; by virtue of being employed or contracted they have forfeited their civilian designation for as long as they are under contract.[154] Civilians who disrupt networks and gather information without express military instruction, but with the military having knowledge of their activities, are likely to be determined as direct participants.[155]

The 'bomb maker' is not directly participating in hostilities as the test of causation is not met.[156] In cyber warfare this is analogous to the person who writes the malware but does not execute it themselves. Current jurisprudence is divided if the 'bomb maker' will be deemed to directly participate in hostilities if it clear that the developed malware is to be used in a situation of warfare.[157] Under traditional warfare, they would not be deemed as directly participating. However, the author believes that the very nature of cyber weapons means that the code will need to modified continuously to react as a weapon.[158] This will require close consultation with military personal and therefore the 'code maker' will know the intention of their output. This involves closer links to the military objectives than under traditional warfare and thus 'code makers' should be considered directly participating in hostilities.[159]

It is the author's submission that the traditional criteria for direct participation needs re-shaping in this jurisdiction to prevent farcical results which would occur under the traditional criteria. All of these features are typical of traditional warfare do not exist in the cyberspace battlefield. Such an example is the international group 'Anonymous' who threatened to attack the United States Pentagon over the Defense

[153] Padmanabhan, above n 16, at 290.
[154] Padmanabhan, as above, at 290; Tallinn Manual, above n 2, at 120; and Crawford, above n 139, at 14-15.
[155] Crawford, as above, at 16.
[156] Crawford, as above, at 16; and Tallinn Manual, above n 2, at 120.
[157] Tallinn Manual, as above.
[158] Padmanabhan, above n 16, at 293.
[159] As above.

Force's detention of Bradley Manning due to his involvement in Wikileaks.[160] They have been behind numerous other large-scale DDOS attacks including recent attacks against the Israeli and Hong Kong governments.[161] As one scholar illustrates:[162]

> If such an operation were launched by an al Qaida cyber unit as part of its armed conflict with the United States, then al Qaida warriors involved in the operation would meet the belligerent nexus requirement [so these civilians would meet the threshold of direct participation in hostilities]. By contrast, members of Anonymous, motivated by free speech concerns, would not, even if their attack would have similarly problematic consequences …

Such a distinction may be justified in traditional warfare where States take action to mitigate the effects, but it seems odd in cyberspace. Anonymous would not fall under LOAC and thus States would only have recourse under domestic criminal law.[163] This situation does not leave attacked States with many effective means of recourse and it is the author's belief that this outcome is amiss.[164]

Conclusions

Cyberspace creates a unique battlefield with many challenges for LOAC. LOAC applies to cyberspace but it is the interpretation of these *jus as bellum* and j*us in bello* principles that are cause of debate. The recently published Tallinn Manual is a useful guide in this area but it is non-binding and does not provide an exhaustive list of instructions. This paper has reflected on a few of the challenges in cyberspace and seeks to conclude these issues below.

It is important to distinguish criminal measures from acts of war. Cyberspace makes this investigation difficult, as the actions to undertake either act are similar. Four methods of attack have been identified: denying access to a network; capturing

[160] At 300.
[161] Jeremy Blum "'Anonymous' hacker group declares cyber war on Hong Kong government, police" (2 October 2014) South China Morning Post <www.scmp.com>; and Dana Liebelson "Inside Anonymous' Cyberwar Against the Israeli Government" (22 July 2014) Mother Jones <www.motherjones.com>.
[162] Padmanabhan, above n 16, at 300.
[163] Watkin, above n 47, at 474.
[164] Padmanabhan, above n 16, at 300.

information; altering or destroying data; and gaining full access of a network. Espionage and warfare both use the same methods. They have been calls for an international treaty to regulate this area but it is unlikely that international consensus would be reached given the current political climate.

States are able to respond in self-defence against armed attacks that violate the Charter's prohibition on the use of force. The application of an armed attack in cyberspace is difficult. Traditionally an armed attack would occur if an attack directly caused injury, death, or damage to property. This criterion is too narrow for the cyberspace jurisdiction. It is the author's contention that an armed attack should include severe data loss as tangible property damage as such damage would cause widespread harm for governments and populations. Financial loss should continue to be excluded from the threshold of an armed attack.

There is a problem of distinguishing targets given the interconnectivity of cyberspace. States are reliant on connected cyber operations for essential services to supply both military and civilian populations including water, electricity, communications and transportation. These dual use targets are deemed military objectives. This rule seems harsh though it must be remembered that such targets will be subject to a proportionality analysis as well as examining whether it is of military necessity to attack and if the attack is severe enough to reach the threshold of an armed attack.

Finally, this paper examined the difficulties with applying the traditional criteria of direct participation to cyberspace hostilities. Cyberspace attackers will not look like traditional combatants. Attackers are unlikely to wear a uniform, openly wear arms, have a commander or be subject to internal disciplinary actions. LOAC needs to widen the traditional criteria for direct participation in cyberspace or perhaps ensure that such inappropriate requirements are waived, such as the requirement to wear a uniform or emblems. Using a strict interpretation of this customary principle, attacked States would not have any right to retaliate against most cyber attackers and it is the author's view that this is an undesirable situation.

BIBLIOGRAPHY

Primary sources

International primary texts

Charter of the United Nations (1945).

Convention on Cybercrime 185 CETS (opened for signature 23 November 2001, entered into force 1 July 2004).

Geneva Conventions 75 UNTS 31 (signed 12 August 1949, entered into force 21 October 1950).

Protocol I Additional to the Geneva Conventions 1125 UNTS 3 (signed 8 June 1977, entered into force 7 December 1978).

Protocol II Additional to the Geneva Conventions 1125 UNTS 3 (signed 8 June 1977, entered into force 7 December 1978).

Protocol III Additional to the Geneva Conventions 2404 UNTS 1 (signed 8 December 2005, entered into force 14 January 2007).

Resolution on the Definition of Aggression GA Res 3314, XXIX (1974).

Domestic primary texts

Computer Fraud and Abuse Act, 18 United States Code.

Police and Justice Act 2006 (United Kingdom).

Secondary sources

Books

Richard Clarke and Robert Knake *Cyber War: The Next Threat to National Security and what to do about it* (HarperCollins Publishers, New York, 2010).

Enrico Fels, Jan-Frederik Kremer and Katharina Kronenburg (eds.) *Power in the 21st Century: International Security and International Political Economy in a Changing World* (Springer-Verlag Berlin Heidelberg, Germany, 2012).

Robert Latham (ed.) *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security* (The New Press, New York, 2003).

Michael Schmitt *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

Dan Verton *Black Ice: The Invisible Threat of Cyber-Terrorism* (McGraw-Hill/Osborne, California, 2003).

Journal articles

Jack Beard "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law" (2014) Vanderbilt Journal of Transitional Law 67.

Laurie Blank "International Law and Cyber Threats from Non-State Actors" (2013) 89 International Law Studies 406.

William Boothby "Methods and Means of Cyber Warfare" (2013) 89 International Law Studies 387.

Ashley Deeks "The Geography of Cyber Conflict: Through a Glass Darkly" (2013) 89 International Law Studies 1.

Yoram Dinstein "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference" (2013) 89 International Law Studies 276.

Louise Doswalk-Beck "Confronting Complexity and New Technologies: A Need to Return to First Principles of International Law" (2012) 106 American Society of International Law 107.

Paul Ducheine and Jelle van Haaster "Fight Power, Targeting and Cyber Operations" (2014) 4 Amsterdam Center for International Law 1.

Robin Geiss "Cyber Warfare: Implications for Non-international Armed Conflicts" (2013) 89 International Law Studies 627.

Duncan Hollis "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" (Beasley School of Law, Temple University) (forthcoming).

Eric Talbot Jensen "Cyber Attacks: Proportionality and Precautions in Attack" (2013) 89 International Law Studies 198.

Jann Kleffner and Heather Harrison Dinniss "Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations" 89 International Law Studies 512.

Noam Lubell "Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?" (2013) 89 International Law Studies 252.

Cassondra Mix "Internet Communication Blackout: Attack Under Non-International Armed Conflict?" (2014) 3 Journal of Law and Cyber Warfare 70.

John Murphy "Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?" (2013) 89 International Law Studies 309.

Vijay Padmanabhan "Cyber Warriors and the *Jus in Bello*" (2013) 89 89 International Law Studies 288.

Michael Schmitt "Classification of Cyber Conflict" (2013) 89 International Law Studies 233.

Michael Schmitt and Liis Vihul "Proxy Wars in Cyberspace: The Evolving International Law of Attribution" (2014) 1 Fletcher Security Review 55.

Nathan Sales "Regulating Cyber-Security" (2013) 107 Northwestern University Law Review 1503.

Paul Walker "Organizing for Cyberspace Operations: Selected Issues" (2013) 89 International Law Studies 341.

David Wallace and Shane Reeves "The Law of Armed Conflict's 'Wicked' Problem: *Levee en Masse* in Cyber Warfare" (2013) 89 International Law Studies 646.

Kenneth Watkin "The Cyber Road Ahead: Merging Lanes and Legal Challenges" (2013) 89 International Law Studies 472.

Matthew Waxman "Cyber Attacks as "Force" under UN Charter Article 2(4)" (2011) 87 International Law Studies 43.

Reports

Bruges Colloquium *Technological Challenges for the Humanitarian Legal Framework* (Delegation of the ICRC to the Kingdom of Belgium, the EU and NATO, 21-22 October 2010).

Paul Ducheine, Frans Osinga and Joseph Soeters (eds.) *Cyber Warfare: Critical Perspectives* (NL ARMS: Netherlands Annual Review of Military Studies 2012).

Jeremy Rabkin and Ariel Rabkin *To Confront Cyber Threats, We must Rethink the Law of Armed Conflict* (Koret-Taube Task Force on National Security and Law, Hoover Institution, Stanford University, 2012).

Dissertations

Wayne Cox "A Crisis 'In' Conflict for International relations: The Case of the Turkish/Kurdish War through Neogramscian Lenses" (Doctor of Philosophy in Political Studies thesis, Queen's University, Kingston, Ontario, Canada, 2000).

Geoffrey Loftus "An Analysis of U.S. Cyberlaw Adaptability and Applications in the Fifth Battlespace" (Master of Science in Cybersecurity thesis, Utica College, New York 2014).

Eric Mifflin "The Law of Armed Conflict in the 21st Century: A Critical Examination of the Legal Relationship between State and Non-State Entities" (Master of Arts in Political Science thesis, University of South Dakota, United States, 2010).

Joe Wesley Moore "Information Warfare, Cyber-Terrorism and Community Value" (LLM thesis, McGill University, Montreal, Canada, 2002).

Internet Resources

Nate Anderson “Confirmed: US and Israel created Stuxnet, lost control of it” (1 June 2012) Arstechnica <http://arstechnica.com>.

Warwick Ashford “Lock up admin accounts to defeat hackers, says Cyber-Ark” (19 June 2013) ComputerWeekly <www.computerweekly.com>.

Jennifer Bjorhus “Group halt bank cyberattacks” (29 January 2013) Star Tribune <http://www.startribune.com>.

Jeremy Blum “’Anonymous’ hacker group declares cyber war on Hong Kong government, police” (2 October 2014) South China Morning Post <www.scmp.com>.

Christopher Bronk “The Cyber Attack on Saudi Aramco” (1 April 2013) Survivial: Global Politics and Strategy <http://www.iiss.org>.

Bill Boothby “UK Armed Forces Personnel and the Legal Framework for Future Operations: Further written evidence from Air Commodore (Retd) Bill Boothy, Doktor Iuris, former Deputy Director of Legal Services (RAF)” (December 2013) United Kingdom Parliament <www.publications.parliament.uk>.

“Denial of Service Attacks” Incapsula <http://www.incapsula.com>.

Tom Espiner “Security experts lift lid on Chinese hack Attacks” (23 November 2005) zdnet.com <http://news.zdnet.com>.

Dan Goodin “Windows driveby attack on aeronautical website may be state sponsored” (21 June 2012) Arstechnica <http://arstechnica.com>.

“Humanity in the Midst of War: Blog related to the laws of armed conflict (LOAC)” (2 October 2012) lawsofarmedconflict.com <http://lawsofarmedconflict.com>.

“Kaspersky Lab Study: about one third of all phishing attacks aimed at stealing money” (2 April 2014) Kaspersky Lab <http://www.kaspersky.com>.

David Kravets “How China’s army hacked America” (20 May 2014) Arstechnica <http://arstechnica.com>.

“International cyber strike attacks US infrastructure” (19 November 2011) The New Zealand Herald <http://www.nzherald.co.nz>.

Ruth Levush “The New Cyber Battlefield: Implications under International Law of Armed Conflict” (10 October 2012) Law Librarians of Congress <http://blogs.loc.gov>.

Dana Liebelson “Inside Anonymous’ Cyberwar Against the Israeli Government” (22 July 2014) Mother Jones <www.motherjones.com>.

Hollie McKay “’Innocence of Muslims’ producer’s identity in question; actors say they were duped, overdubbed” (13 September 2012) Fox News <http://www.foxnews.com>.

Phil Muncaster “India to greenlight state-sponsored cyber attacks” (11 June 2012) The Register <http://www.theregister.co.uk>.

Anna Nelson “What everyone needs to know about cyber warfare” (15 May 2014) Intercross <http://intercrossblog.icrc.org>.

New Zealand Government “New Zealand’s Cyber Security Policy” (June 2011) Department of the Prime Minister and Cabinet <www.dpmc.govt.nz>.

Pierluigi Paganini “Nation state sponsored attacks: the offensive of Governments in cyberspace” (12 November 2012) Security Affairs <http://securityaffairs.co>.

Pierluigi Paganini “State-sponsored attack or not, that’s the question” (18 September 2012) Security Affairs <http://securityaffairs.co>.

Leon Panetta “Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City” (11 October 2012) United States Department of Defense <http://www.defense.gov>.

Douglas Rushkoff “Extreme response not a solution” (17 July 2002) The Guardian <http://www.theguardian.com>.

“Roundtable on Cyberwar and the Rule of Law” (15 October 2012) University of Pennsylvania Law School <www.law.upenn.edu>.

“The law of war imposes limits on cyber attacks too” (1 July 2013) International Committee of the Red Cross <www.icrc.org>.

Ian Traynor "Russia accused of unleashing cyberwar to disable Estonia" (17 May 2007) The Guardian <http://www.theguardian.com>.

"Weapons: ICRC statement to the United Nations" (16 October 2013) International Committee of the Red Cross <www.icrc.org>.

"What limits does the law or war impose on cyber attacks?" (28 June 2013) International Committee of the Red Cross <www.icrc.org>.

"Why Russia is taking on the West over Cyber Warfare" (6 November 2013) Worldcrunch <http://www.worldcrunch.com>.

Other Resources

James Adkisson and others *Law of Armed Conflict: Implications for Navy Cyber Strategy* (Masters of Information Technology Strategy Practicum – 2012, Carnegie Mellon University, Pittsburgh, Pennsylvania, 3 August 2012).

Emily Crawford *Virtual Battlegrounds: Direct Participation in Cyber Warfare* (Legal Studies Research Paper No. 12/10, Sydney Law School, The University of Sydney, February 2012).

Michael Schmitt (ed). *DRAFT Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).