# Evolution of the Battlefield: strategic and legal challenges to developing an effective cyber warfare policy

**Sub Lieutenant Nam Nguyen, RAN**

It is better to be vaguely right than exactly wrong.

Carvath Read, *Logic: deductive and inductive*, 1898 [1]

## Introduction

In the 21st century, governments, businesses and individuals are increasingly reliant on information and communication technologies (ICT) for large transactions and to support critical national infrastructure. As much as this technology has made daily life more convenient, there is significant risk associated with these systems, not least because individuals, groups and state-sponsored actors (as well as states themselves) have found ways to manipulate or 'hack' into these systems to further their own objectives.

This, of course, has significant follow-up consequences on how ICT is used as part of a government's arsenal to protect its national interests. While it is important to consider the use of cyber capabilities more broadly in the context of national security, particularly their effects on international reputation and diplomatic relations, it is even more important to examine their potential effects when used in armed conflict, including their impact on the civilian populace and where loss of life may occur.

This article argues that significant work needs to be done in this area, especially since most developed states, including Australia, have insufficient publicly-available strategies and policy positions on dealing with cyber threats.[2] Policy makers and military planners must be aware that part of every conflict will take place in cyber space, which can be just as important, 'if not more so, than events taking place on the ground'.[3]

The article examines existing and potential cyber capabilities and how they may be used in armed conflict. Classic strategic thought provides some guidance. These maxims, however, only provide overall logic for how cyber warfare can be used to achieve policy aims. Moreover, the legality of cyber warfare actions are a point of contention among academics, policy-makers and military planners, with a number of grey areas as to 'when and how' cyber means may be employed in armed conflict.

Significant work has been done to alleviate this area of contention. The *Tallinn Manual* on the international law applicable to cyber warfare, produced by NATO's Cooperative Cyber Defence Centre of Excellence (located at Tallinn, Estonia),[4] provides non-binding guidance on the use of cyber capabilities during armed conflict.[5] However, it only applies when it has been determined that an international armed conflict has commenced, leaving open the need to further develop broader and more general cyber laws applicable at an international level.

There are numerous cases where cyber means have been deployed in support of conventional operations, which can be particularly useful case studies for analysing the strategic and legal implications of cyber warfare. Developing potential scenarios and 'war gaming' their resolution can also be useful in giving analysts and practitioners the ability to explore a range of cyber warfare-related considerations. Unfortunately, this can prove difficult when experts in the field find it difficult to reach consensus on an exact definition of cyber warfare, as well as the capabilities involved, and the extent to which it can or should be considered a separate domain to land, sea and air.

## What is cyber warfare?

Clearly-defined concepts are useful for constructing propositions, theories and analytical frameworks.[6] One of the difficulties in developing an effective framework for cyber warfare doctrine is that its

definition is either incomplete or too broad. There also remains significant debate over what constitutes cyber warfare, beyond the cyber methods or the 'how-to' of achieving policy aims in cyberspace.[7] The 'pro-cyber war' camp claims that cyber space is a real domain and an unavoidable security issue, contending that governments and militaries should be ready for an eventual and unavoidable future cyber war. On the other hand, those on the 'anti-cyber war' side argue the threat has been overstated, overused and hyped for no reason, and that a distinct cyber war is unlikely.[8]

Even so, most involved in the debate are not working on a universal definition of 'cyber warfare'—let alone the related terminology—as illustrated by the following:

- 'Information war' is a 'confrontation between two or more States in the information space aimed at … undermining political, economic, and social systems … or mass psychologic [sic] brainwashing to destabilize society and State'.[9]

- A cyber attack is 'the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social, ideological, religious, political or similar objectives; or to intimidate any person in furtherance of such objectives'. [10]

- 'Cyber power' is the ability to obtain preferred outcomes through the use of the electronically-interconnected information resources of the cyber domain.[11]

- 'Cyber warfare' is 'the use of network-based capabilities of one state to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves, of another State'.[12]

- 'Cyber warfare' occurs 'when one country perpetrates a cyber attack against another country that would, to the reasonable person, constitute a State act of war'.[13]

- 'Cyber operations' include 'the protection of deployed networks and information systems' against an adversary using a cyber attack against Australia 'to deter, delay or prevent Australia's response or the ADF's deployment of forces. This would probably include the targeting of information systems, networks and broader support infrastructure perceived to be integral to the ADF's decision-making and warfighting capabilities'.[14]

These examples demonstrate the varied definitions of cyber operations and/or cyber attacks. The first, focusing on cyber operations in the information space between states, seemingly overlooks the involvement of non-state actors. Similarly, the first-mentioned definition of cyber warfare seems to focus too narrowly on computers and their networks. Others focus on particular critical components but none, for example, includes methods of attack.

Most people have a broad idea as to what can be done with cyber capabilities. The internet's imperfect design enables hackers to read, delete or modify information between computers. Additionally, the maze-like architecture of 'the web' allows those with malicious intent a degree of anonymity that is generally not available in physical attacks on infrastructure or persons, facilitating obscurity and a degree of deniability.[15]

There are, however, more provocative uses for these methods beyond causing inconvenience for political purposes. Cyber espionage has the same purpose as the traditional form of espionage, only now it can be conducted using illegal exploitation methods through the internet, networks, software or computers. Another method of cyber attack is a 'denial-of-service' attack, whose purpose is to deny the use of a computer or network, which can be achieved by flooding a target with superfluous data or physically destroying the computer's software.

A third type of cyber attack is data manipulation or sabotage. The most common means of conducting these attacks are through malicious software programs (malware), which can alter the code within computer networks and programs. Less severe forms of this method cause a degree of inconvenience, as was seen in late 2013 when Indonesian hackers defaced the Australian Secret Intelligence Service's public

website.[16] That, however, was a relatively benign example of cyber sabotage. Data modification can also be extremely dangerous because 'a successful attack can mean that legitimate users (human or machine) will make important decisions based on maliciously altered information', which could corrupt command and control systems or even allow the takeover of those systems.[17]

The potential to use cyber space as a medium to conduct warfare is clear. But defining what constitutes cyber warfare is considerably more problematic. Moreover, some would argue that developing a single definition of cyber warfare carries inherent risks, as 'focusing on one aspect of cyber space creates a strategic and conceptual blind spot…. It also has a tendency to focus consideration of risk via threats and vulnerabilities on transmission mechanisms'.[18]

Similarly, military planners may make the mistake of thinking of cyber warfare as merely a decisive, tactical and information-enabled force multiplier in the aid of conventional warfare.[19] Thus developing a concise definition of cyber warfare may actually restrict armed forces from being able to develop doctrine that is both effective in achieving the stated aims of government policy and flexible enough to allow military planners to develop ways to counter emerging threats.

## War, doctrine and cyber policy

Despite the lack of internationally-recognised definitions, there is sufficient material to be able to discern the unique characteristics of cyber warfare. Broadly speaking, these characteristics are speed, anonymity and flexibility of the systems. These characteristics can present a significant challenge because 'planning and preparing for a [cyber] attack may take weeks or more to develop … but, once launched … may well be over in a matter of seconds. Consequently, in many cases we may not realistically be able to react to an attack in progress'.[20]

Furthermore, rather than wearing down an adversary's defences, cyber warfare can be used to bypass conventional defences 'in order to penetrate the adversary's system and exploit it through speed and surprise'.[21] As was seen during the Russia-Georgia conflict in 2008, hackers were able to cripple Georgia's internet communications networks, which had significant flow-on consequences for Georgia's command and control capability.[22] While it can be expected that many states will similarly use cyber methods to shape the future battlespace, particularly against a technology-dependent adversary, the full potential of cyber warfare in armed conflict has arguably not yet been realised.[23]

Throughout history, whenever there has been a 'revolution in military affairs and technology', it has always been followed with a strategic effect.[24] The problem with the cyber warfare debate is that there are very few examples of how cyber means have been employed in support of and during armed conflicts. Even then, some of these examples have issues of attribution, such as the Stuxnet virus attack on Iranian nuclear facilities, which makes it difficult to study the full extent of this new mode of warfare.[25]

Perhaps an examination of the classic strategists, Carl von Clausewitz and Basil Liddell Hart, can provide some guidance on how best to perceive the threat of cyber warfare and how to use these new capabilities, thus assisting to develop appropriate doctrine and policy.

Adopting a Clausewitzian view of strategy will assist governments and military planners to determine what it is they wish to achieve and by what means they will measure their success.[26] Particularly as the vulnerabilities in cyberspace become apparent, understanding the underlying intent of such capabilities, and their purpose, can aid in determining their employment. Clausewitz also talks about the concept of an enemy's centre of gravity (and, as a consequence, one's own centre of gravity) as being the linkages that allow the enemy to wage war.[27]

Whichever definition is used, the essential element is the dominant characteristic (strength) of either party. In the case of cyber warfare, the more 'electronically dependent an actor is, the more vulnerable it is'.[28] Thus it would be prudent for military planners to examine their own weaknesses in order to determine how best to employ cyber means against an adversary.

The maxims of other classical strategic thinkers would point to a similar course of action. Liddell Hart describes strategy as the 'art of distributing and applying military means to fulfil the ends of policy'.[29] Helmuth von Moltke calls it 'the practical adaptation or the means placed at a general's disposal to the

attainment of the object in war'.[30] Like Clausewitz, however, these two definitions focus on the relatively narrow view of how military force can achieve a political aim. Given that the use of military force is rarely used in isolation, strategy in the modern context must be expanded to include other means.[31] As Robert Osgood suggests:

> Strategy must now be understood as nothing less than the overall plan for utilising the capacity for armed coercion—in conjunction with economic, diplomatic, and psychological instruments of power—to support foreign policy most effectively by overt, covert, and tacit means.[32]

This definition provides a broader focus on power and the fundamental nexus between the military aspect and foreign policy goals. It also takes into account national objectives and acknowledges that strategy is not a purely militaristic endeavour. Along these lines, a 'grand strategy' for cyber warfare would encompass all aspects of national power in order to develop doctrine that can be employed by all arms of government.

## The ethical dimension and the law of armed conflict

The challenge in developing a clear and concise cyber strategy is determining the distinction between day-to-day security issues (such as managing cyber crime) and matters governed by the laws of armed conflict.

One document that provides comprehensive analysis of extant legal norms is the previously-mentioned *Tallinn Manual*. However, even though it provides some clarity on the application of international law to cyber conflicts, there are still key areas that require further discussion. For example, its editor concedes that 'crafting a consensus understanding of [the] definition of "attacks"… proved arduous'.[33] Similarly, the experts involved could not agree on what constitutes 'war-sustaining' military objectives for legitimacy of targeting.[34] This is particularly important when considering that an attack by cyber means could result in a response involving the use of kinetic weapons.[35]

Put simply, there is no clear guidance as to when states can respond to a cyber attack with armed force, notwithstanding what may seem to be clear examples of legitimate targets in the spectrum of cyber warfare. For example, in the Russo-Georgian conflict in 2008, Moscow presumably perceived Georgia's computer networks as legitimate targets because of their role in supporting attacks on Russian troops.[36]

This, however, is a 'neat' example of where a response can be considered lawful, as both actors were states operating in the context of an international armed conflict. The experts involved in the preparation of the *Tallinn Manual* suggested that states should consider the intended effect of a cyber operation; more specifically, they argued that the physical effects of a cyber attack, and whether it results in death or damage to civilian objects, should guide the appropriate response.[37]

As highlighted earlier in this article, there is also no clear definition of a cyber weapon. The *Tallinn Manual* does not specify what would constitute such a weapon, other than discussing its characteristics, nor does it make any definitive conclusions regarding them.[38] Despite this, the experts agreed that existing protocols of the Geneva Convention are sufficient to address the requisite procedures for assessing any new, cyber-related weaponry and their application in armed conflict, effectively rejecting any characterisation of the cyber domain as being subject to a discrete body of law that was yet to be developed.[39]

Perhaps a close study of some of the 'cardinal' principles of the law of armed conflict could provide some further guidance into the use of cyber weapons in armed conflict. Consider, for example, the principle of 'distinction', which relates to the capacity of weapons to distinguish between civilian and military targets.[40] In an opinion expressed in the International Court of Justice, Justice Rosalyn Higgins defined weapons that were unable to distinguish between civilian and military targets as 'blind'.[41] In the case of cyber warfare, it is conceivable that malware, for example, may be coded only to attack military objectives. On the other hand, the practitioners that developed the code could deliberately or otherwise overlook such fail-safes and create a cyber weapon that is effectively 'blind' in its targeting.

The principle of distinction also raises further strategic consequences worth considering in the cyber debate, apart from international humanitarian law concerns. The features of this new cyber domain, such

as the interconnectivity of computer networks, bring significant utility to states and societies during peacetime. Much of the development in ICT has been a result of business and industrial innovation, and the national security community has benefited from this immensely. Indeed, states should recognise the strategic importance of critical ICT infrastructure to national survival today, just as other forms of infrastructure did almost a century ago.[42]

During times of armed conflict, however, the ability to prevent significant collateral damage to the civilian population may be hampered by the interconnectedness of military networks and their reliance on civilian infrastructure.[43] During the 1990-91 Gulf War, for example, a coalition attack on Iraq's electricity grid successfully disrupted its military command and control networks; however, an unintended consequence was that the attack impacted the civilian population, including through its effect on emergency services.[44]

Anonymity in cyberspace is a further impediment to regulating cyber weapons and their use in armed conflict. While many commentators believe the Stuxnet virus could only have been developed by an organisation backed by considerable state-level resources,[45] no country or organisation has claimed responsibility for the attacks and computer forensic investigation has failed to conclusively attribute the virus to any state.[46] A further complication arises in the *Tallinn Manual's* assertion that 'the mere fact that a cyber operation has been launched … from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that State'.[47] This raises significant questions for those who fall victim to a cyber attack, and their right to an armed response in self-defence.[48]

Moreover, even if successful attribution of a cyber attack to a belligerent state (or state-sponsored group) is achieved, the fundamental principles of the law of armed conflict may prevent or complicate a cyber response. Heather Dinniss argues that armed force in self-defence is only a legitimate course of action if used to repel an attack when other non-forcible remedies have proven unsatisfactory.[49] Others argue that any response under the principle of military necessity should be made without undue delay, suggesting that even if states are able to identify where a cyber attack originated, the legality of an armed response may be jeopardised by the time it takes to launch a counter-attack.[50]

The potential strategic gains from cyber warfare may influence states to attempt to blur international humanitarian law and the law of armed conflict applying to cyber war. One solution that has been suggested is to adopt a consequence-based approach to cyber attacks, rather than attempting to apply the relevant international law.[51] This is because, as previously mentioned, not all malicious cyber activities can be considered 'armed attack'.[52]

Consider, for example, a hypothetical NATO-led bombing strike against a state-owned television station being used as a military communications centre.[53] The majority of the television station's day-to-day activities would likely be non-military and involve a number of civilians with no direct role in military activities. Hence, an airstrike aimed at knocking out the communications network would carry the risk of significant civilian casualties. However, a cyber attack could likely achieve the same endstate, with no risk of casualties or physical damage and minimal risk of international approbrium.

## A global effort: towards a cyber treaty?

A number of commentators have called for serious discussion to better delineate the line between cyber warfare and traditional warfare,[54] not least because 'cyber warfare is coming of age in an era where the Westphalian state order is undergoing vast transformation'.[55] Traditional ideas of borders and sovereignty only serve to complicate discussion and a truly international effort should be explored in order to ensure consensus over the issues discussed in this article.

Additionally, beyond the strategic and humanitarian considerations for developing a cyber warfare doctrine, the unique nature of cyber space must be taken into consideration. Cyber space transcends traditional boundaries and this fact only adds to the 'grey area' in this debate, particularly when determining the difference between cyber crimes and cyber attacks which could be interpreted as acts of war.

What arguably is required is an overarching international treaty regulating the use of cyber weapons in all instances, rather than just for internationally-recognised armed conflicts. Existing international laws

support coercive measures (though not armed attacks) in order to respond to economic wrongs and the violation of arms control treaties by states. So consideration should be given to extending these rules to the use of cyber weapons.[56]

In the economic domain, state responses to violations are known as 'counter-measures' and in the arms control domain they are called 'sanctions'.[57] Both are coercive methods of enforcement which do not necessarily require the use of military force.[58] This is a particularly important consideration because useful lessons can be drawn from existing arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, to address how specific types of weaponry may or may not be used in both armed conflict and peacetime.[59] Having a separate cyber space or cyber weapons treaty could serve not only to clarify how these tools may be employed but also to maintain the viability of the cyber domain for peaceful purposes.

Not everyone in the international law community, however, supports the view that a distinct cyber treaty is required. Some argue that treaties are not the answer, and that norms regarding the use of cyber weapons should, and will, evolve through customary law, codes of conduct, and rules of engagement.[60] Others similarly suggest this is because states will actively 'avoid prematurely limiting a weapon that could potentially offer some measure of non-lethality to conflict'.[61]

It has also been suggested that while a ban or treaty might be logical to prevent unforeseen consequences, its application may be unrealistic.[62] There are two reasons advanced in support of this argument. Firstly, many cyber capabilities and networks are dual-purpose and have peaceful utility for non-military purposes.[63] Secondly, a treaty may regulate the behaviour of states but will not necessarily prevent non-state actors from breaching the principles of the treaty. This is because smaller states and politically-motivated groups may seek to enhance their cyber capabilities as a force multiplier against more powerful opponents.

Perhaps a further barrier to developing a body of law that governs cyber warfare is the fact that the full effects of cyber weapons have not been seen. This has been a point of contention emphasised throughout this article. Unlike land mines or nuclear weapons (which ultimately led to the Ottawa Treaty and the Nuclear Non-Proliferation Treaty), it is difficult to assess where to draw the line in regulating cyber weaponry. One assessment of the difficulties in reaching consensus on an international cyber weapons treaty is that:

> Visible or readily discernible state practice is still scarce. The military potential of computer network attacks is now only starting to be fully explored, and it is difficult to assess how realistic or likely the theoretical worst-case scenarios that are contemplated in the literature—for example, the manipulation of a nuclear power plant via cyber space—really are.[64]

Hence, there is obvious merit in pursuing internationally-accepted norms rather than trying to enforce an international treaty.[65] However, there are even greater risks associated with failing to develop an internationally-binding code or treaty on cyber space and cyber weapons as, without an overarching framework to guide states on the use of cyber weapons, the proliferation of even more devastating cyber weapons could become possible. Given that there is little agreement in relation to current capabilities, states and non-state actors and other groups may be driven to prepare for worst-case scenarios, or engage in tit-for-tat escalation, as occurred in the early days of the Cold War nuclear arms race.[66]

## Conclusion

In contemplating the future, analysts and theorists can debate worst-case scenarios and try to assess likely courses of actions by states. Perhaps a cyber attack that shocks the consciousness of humanity will prompt further insight into how best to regulate cyber weapons. The potential advantages of cyber warfare, however, may be an incentive for states to avoid developing a framework that is too restrictive.

This means that due diligence is required when proceeding with the development of cyber strategies and tactics. States need to consider the impact of this new form of warfare, not just from a legal and strategic perspective, but also because of the ethical implications of employing these means against civilians, protected persons and objects. It may be that cyber weapons will eventually become more prominent in armed conflicts. After all, the ability to achieve the same effects as kinetic weapons, without the

associated damage to objects or civilian casualties, will likely prove particularly enticing to decision-makers.

It is without question that more needs to be done to prepare for cyber space and how cyber weaponisation will affect international relations and warfare generally. A cyber attack on a nation's financial institutions would be disastrous. But the effects are potentially reversible. On the other hand, poor or untimely decisions by military practitioners and states using kinetic weapons may lead to unnecessary loss of life and other irreversible collateral damage.

The quote at the beginning of this article neatly summarises the dilemma that governments and military planners face moving forward in the cyber warfare debate. The *Tallinn Manual* and existing literature on the topic provides insight as to how cyber warfare may be used and regulated but there are limits to that guidance when used to develop policy. This raises significant legal, ethical and strategic questions to consider when determining the future application of cyber weapons.

Even the 'cardinal principles' of the law of armed conflict, and the guidance of classical strategic thinkers, do not provide a definitive answer. It is clear from the literature that there is no consensus on the way forward in terms of regulating the use of cyber weapons, particularly in relation to international humanitarian law. There are arguments in favour of international treaties and arguments that support the idea of international norms to regulate the use of cyber weapons in armed attacks. Future policies will need to address both sides of this debate.

Cyber weapons can prove useful for militaries in future but the aim should be to focus on minimising damage to civilians. Governments and military planners need to examine every facet of this new domain in a timely fashion to develop the most appropriate doctrine or policy. Failure to do so may result in a focused cyber attack that truly shocks the conscience of humanity.

*Sub Lieutenant Nam Khoa Nguyen is a Maritime Warfare Officer in the RAN. He is a graduate of ADFA and has a Bachelor of Business degree. In 2013, Nam was the ADF delegate to 'Global Voices', a not-for-profit organisation seeking to promote an understanding of and participation in international diplomacy by young Australians. He has previously served at sea onboard HMA Ships Kanimbla and Labuan. Nam is currently posted to HMAS Watson to complete Phase IV Junior Warfare Application Course.*

## NOTES

1 This quote is often misattributed to Keynes. The original quote comes from Carvath Read, *Logic: deductive and inductive,* 1st Edition, Grant Richards: London, 1898, p. 351, available at <http://www.gutenberg.org/files/18440/18440-h/18440-h.htm#Page_351> accessed 21 September 2014.

2 T. Feakin, J, Woodall and K. Aiken, 'Cyber Maturity in the Asia-Pacific Region', Australian Strategic Policy Institute, International Cyber Policy Centre: Canberra, 2014, available at <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf> accessed 30 September 2014.

3 K. Geers, 'Cyberspace and the changing nature of warfare', *SC Magazine* (online), 27 August 2008, available at <http://www.scmagazine.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/> accessed 17 October 2014.

4 See <https://ccdcoe.org/tallinn-manual.html> accessed 2 March 2015.

5 See M. Schmitt (ed.), *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge University Press: Cambridge, 2013, available at <https://ccdcoe.org/tallinn-manual.html> accessed 12 January 2015.

6 D.A Baldwin, 'The concept of security', *Review of International Studies,* Vol. 23, 1997, pp. 5-26.

7 The term 'cyber methods' refers to the use of computers, networks and malicious software (malware). It does not refer to operational employment and/or concepts but is used to describe the basic requirements for launching a cyber operation. The threshold for determining a weaponised cyber method is not clearly defined in law.

8 H. Mehmetcik, 'A New Way of Conducting War: cyberwar, is that real?', in J-F. Kramer and B. Muller (eds.), *Cyberspace and International Relations: theory, prospects and challenges,* Springer: New York, 2013, pp. 125-39.

9 T. Gjelten, 'Shadow Wars: debating cyber disarmament', *World Affairs,* Vol. 173, No. 4, 2010, p. 36.

10 Kevin Coleman, 'Cyber Terrorism', *Directions Magazine*, 10 October 2003, available at <http://www.directionsmag.com/article.php?article_id=432> accessed 15 October 2014.

11 J.S. Nye Jr., *Cyber Power*, Belfer Center for Science and International Affairs, Harvard Kennedy School: Cambridge, 2010, pp. 3-4.

12 A.J. Schapp, 'Cyber warfare operations: development and use under international law', *Air Force Law Review,* Vol. 64, pp. 121-74.

13 D.B. Garrie, 'Cyber Warfare: what are the rules?', *Journal of Law & Cyber Warfare,* Vol. 1, No. 1, 2012, pp. 1-7.

14 Department of Defence, *Defence White Paper 2013,* Australian Government: Canberra, 2013, p. 20.

15 K. Johnson and D.L. Leger, 'US accuses China of Cyber Espionage', *USA Today*, 19 May 2004, available at <http://www.usatoday.com/story/news/nation/2014/05/19/us-accuses-china-of-cyber-espionage/9273019/> accessed 30 September 2014.

16 F. Foo, 'Hackers cripple ASIS website', *The Australian*, 12 September 2013, available at <http://www.theaustralian.com.au/technology/hackers-cripple-asis-website/story-fn4htb9o-1226757688241> accessed 15 October 2014.

17 Geers, 'Cyberspace and the changing nature of warfare', 2008.

18 S.E. Liles, 'An Argument for a Comprehensive Definition of Cyberspace,' Selil (blog), 18 November 2011, available at <http://selil.com/archives/2712> accessed 3 October 2014.

19 A. Sharma, 'Cyber Wars: a paradigm shift from means to ends' in C. Czosseck and K. Geers (eds.), *The Virtual Battlefield: perspectives on cyber warfare,* Cryptology and Information Security Series, Vol. 3, IOS Press BV: Amsterdam, 2009, pp. 3-17.

20 S.C. Butler, 'Refocusing Cyber Warfare Thought', *Air & Space Power Journal,* January-February 2013, pp. 50-1.

21 T.E. Mitchell, 'Cyber Warfare: supporting MEU operations', *Marine Corps Gazette,* Vol. 98, No. 2, 2014, pp. 44-7.

22 See, for example, J. Markoff, 'Before the Gunfire: cyberattacks', *New York Times*, 12 August 2008, available at <http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0> accessed 12 January 2015.

23 C.B. Greathouse, 'Cyber War and Strategic Thought: do the classic theorists still matter?' in Kramer and Muller, *Cyberspace and International Relations*, pp. 21-37.

24 Sharma, 'Cyber Wars', p. 5.

25 See, for example, Ellen Nakashima, 'Stuxnet worm targeting Iran in works as early as 2005, Symantec finds', *The Washington Post*, 26 February 2013, available at <http://www.washingtonpost.com/world/national-security/stuxnet-worm-targeting-iran-in-works-as-early-as-2005-symantec-finds/2013/02/26/4cb562d8-8059-11e2-8074-b26a871b165a_story.html> accessed 12 January 2015.

26 A. Stephens and N. Baker, *Making Sense of War: strategy in the twenty-first century*, Cambridge University Press: Cambridge, 2006, pp. 260-1.

27 Stephens and Baker, *Making Sense of War,* pp. 485-6.

28 A. Liaropolous, 'Cyber-Security and the Law of War: the legal and ethical aspects of cyber-conflict', Working Paper No. 7, Greek Politics Specialist Group, Piraeus University: Greece, 2011, p. 4, available at <http://www.gpsp.prg.uk/docs/GPSC_Working_Paper_7.pdf> accessed 12 January 2015.

29 J. Baylis, J.J. Wirtz and C.S. Gray, *Strategy in the Contemporary World,* 4th Edition, Oxford University Press: Oxford, 2013, pp. 4-5.

30 Baylis, Wirtz and Gray, *Strategy in the Contemporary World*, pp. 4-5.

31 M.L. Cook, 'Ethical issues in War, An Overview', in Joseph R. Cerami and James F. Holcomb (eds.), *US Army War College guide to strategy,* Strategic Studies Institute: Carlisle, 2001, pp. 19-30.

32 Baylis, Wirtz and Gray, *Strategy in the Contemporary World,* p. 5.

33 Baylis, Wirtz and Gray, *Strategy in the Contemporary World*, p. 17.

34 Baylis, Wirtz and Gray, *Strategy in the Contemporary World*, p. 17.

35 D. Fleck, 'Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual', *Journal of Conflict & Security Law,* Vol. 18, No. 2, March 2013, p. 337.

36 M.E. O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, pp. 192-3.

37 M.N. Schmitt, 'International Law in Cyberspace: the Koh Speech and Tallinn Manual juxtaposed', *Harvard International Law Journal,* Vol. 54, December 2012, p 19.

38 In the *Tallinn Manual*, the 'means of cyber warfare' are somewhat vaguely defined only as cyber weapons and their association with cyber systems: see Schmitt, *Tallinn Manua*l, pp. 141-2.

39 Schmitt, 'International Law in Cyberspace', p. 17.

40 Y. Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, p. 262.

41 International Court of Justice, 'Dissenting Opinion of Judge Higgins, Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)', 1996, available at <http://www.icj-cij.org/docket/files/95/7525.pdf> accessed 20 September 2014.

42 An analogy can be drawn between security analysts' fear of the onset of airpower and recent debate regarding cyber warfare: see M.S. Sherry, *The Rise of American Air Power,* Yale University Press: New Haven, 1987, p. 36.

43 R. Geib, 'The Conduct of Hostilities in and via Cyberspace', War and Law in Cyberspace Panel, *American Law in Society Proceedings*, 2010, p. 372.

44 For a similar situation, see BBC, 'NATO Denies Targeting Water Supplies', BBC World Online Network, 24 May 1999, available at <http://www.news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm> accessed 3 October 2014. In this situation, a NATO air strike targeted Yugoslavia's electrical supply network during Operation ALLIED FORCE. One consequence of that attack was the shutdown of pumping stations, disrupting the supply of fresh water to civilians.

45 J. Fildes, 'Stuxnet Work "Targeted high-value Iranian Assets"', *BBC News,* 23 September 2010, available at <http://www.bbc.co.uk/news/technology-11388018> accessed 30 September 2014.

46 H.H. Dinniss, *Cyber Warfare and the Laws of War,* Cambridge University Press: New York, 2012, p. 291.

47 Schmitt, *Tallinn Manual*, 'Rule 7', pp. 34-5.

48 See Article 51 of the UN Charter, available at <http://www.un.org/en/documents/charter/chapter7.shtml> accessed 12 January 2015.

49 Dinniss, *Cyber Warfare and the Laws of War*, p. 102.

50 Y. Dinstein, *War, Aggression and Self-Defense*, 3rd Edition, Cambridge University Press: New York, 2001, p. 210.

51 M.N. Schmitt, 'Wired Warfare: computer network attack and *jus in bello*', *International Review of the Red Cross,* Vol. 84, No. 846, 2002, pp. 374-5.

52 Schmitt, 'Wired Warfare', pp. 374-5.

53 This scenario was adapted from an actual NATO airstrike against Serbian state television in April 1999: see Schmitt, 'Wired Warfare', pp. 381-2.

54 See, for example, A.M. Colarik & L. Janczewski, 'Establishing Cyber Warfare Doctrine', *Journal of Strategic Security,* Vol. 5, No. 1, 2012, pp. 31-48.

55 R. Hughes, 'Towards a Global Regime for Cyber Warfare' in Czosseck and Geers, *The Virtual Battlefield,* p. 110.

56 O'Connell, 'Cyber Security without Cyber War', p. 203.

57 N. White and A. Abass, 'Countermeasures and Sanctions' in M. Evans (ed.), *International Law,* 3rd Edition, Oxford University Press: Oxford, 2010, p. 531.

58 O'Connell, 'Cyber Security without Cyber War', p. 203.

59 O'Connell, 'Cyber Security without Cyber War', p. 205.

60 J.T.G. Kelsey, 'Hacking into International Humanitarian Law: the principles of distinction and neutrality in the age of cyber warfare', *Michigan Law Review,* Vol. 106, 2008, pp. 1449-50.

61 B.W. Ellis, 'The International Legal Implications and limitations of Information Warfare: what are our options?', Strategy Research Paper, US Army War College: Carlisle, 2001, p. 14.

62 Ellis, 'The International Legal Implications and limitations of Information Warfare', p. 14.

63 Ellis, 'The International Legal Implications and limitations of Information Warfare', p. 14.

64 Geib, 'The Conduct of Hostilities', p. 372.

65 The panel of experts agreed to similar points of discussion when drafting the *Tallinn Manual*.

66 J.H Herz, 'Idealist Internationalism and the Security Dilemma', *World Politics,* Vol. 2, No. 2, 1950, pp. 157-80.