The International Humanitarian Law Implications of the 'Tallinn Manual'

https://www.e-ir.info/2014/02/12/the-international-humanitarian-law-implications-of-the-tallinn-manual/

NAM KHOA NGUYEN, FEB 12 2014

The International Humanitarian Law Implications of the Tallinn Manual on the International Law Applicable to Cyber Warfare

*'It is better to be vaguely right than exactly wrong.'— John Maynard Keynes**[1]***

Introduction

The Tallinn Manual on the International Law Applicable to Cyber Warfare (hereon referred to simply as 'The Tallinn Manual') is the result of a three-year effort to assess how current international laws apply to this 'new' form of warfare.[2] It critically assesses the *jus ad bellum* and *jus in bello* laws governing the use of cyber capabilities by States in armed conflicts.[3] The Tallinn Manual is a non-binding document and aims to provide some guidance (what the group of experts call 'rules') on the use of cyber technology during armed conflict.

Although related bodies of international humanitarian law (IHL), such as the law of sea, are dealt with in the manual, the document raises more questions about cyber warfare in future conflicts, than it does provide answers.[4] Evaluating cyber warfare through the cardinal principles of the law of armed conflict (LOAC) may provide some clarity, but even this still raises some significant issues concerning strategic and ethical implications of the Tallinn Manual and cyber warfare.[5] Despite not being the panacea for international law on cyber warfare, the Manual still provides a foundation to assess the legality of cyber warfare in international and non-international armed conflict. This means that States still have a relevant source to use when analysing the impact of their cyber response so that the impact on civilians can be minimised.[6]

The Tallinn Manual and IHL

Critics of the Tallinn Manual, such as Dieter Fleck, suggest that the Manual's greatest contribution to IHL is that it has proven extant international humanitarian laws still apply to cyber warfare.[7] Since the purpose of the Tallinn Manual was to assess whether international law applied to cyber conflict, it can be argued that the Manual achieved its purpose.[8] This is important as it provides States with a basis to frame their response during international or non-international armed conflict. However, even though the Manual provides some clarity to the applicability of international law to cyber conflicts, there are still key areas that even the Manual recognises as requiring further discussion. For example the editor of the Tallinn Manual, international law scholar Michael Schmitt, concedes that even 'crafting a consensus understanding of (the) definition of "attacks"… proved arduous.'[9] Similarly, the experts could not agree on what constitutes 'war-sustaining' military objectives for legitimacy of targeting.[10] This is particularly important considering that an armed conflict triggered by cyber means may result in States escalating to using kinetic weapons.[11]

Although the Tallinn Manual applies extant laws for States to follow when considering the use of cyber weapons, there still exists the potential for miscalculation to occur in interpreting the *jus ad bellum.* Put simply, when should one respond with force to a cyber attack? International dispute lawyer, Mary O'Connell, provides an example of

Russian forces launching a cyber attack on Georgian computer networks, that are directly linked to computer networks used to support an attack on Russian troops, as a legitimate target during armed conflict.[12] This, however, is a 'neat' example of when a response in force is lawful; both actors are States operating within the context of an agreed international armed conflict. The international group of experts suggested that States should consider the effects of a cyber operation if there is confusion about what would constitute a lawful response. More specifically, the *physical* effects of cyber operations on the civilian population, and whether it results in death or damage to civilian objects, should guide the appropriate force response.[13]

The Tallinn Manual does not specify what means would constitute a cyber 'weapon', nor does it attempt to make any definitive conclusions on them.[14] Essentially, the characteristics of what a cyber weapon is are discussed but the experts do not offer a definitive list of 'cyber weapons'. Despite this, the international group of experts agreed that, despite not being able to categorise the types of cyber weapons available in armed conflict, the conditions set by Article 36 of Additional Protocol I (AP 1) of the Geneva Conventions would sufficiently cover the requisite procedures for assessing new weaponry.[15] [16] By referring to AP I as the basis for reviewing new forms of cyber weapons, the experts agree that preexisting law applies to cyber warfare, and reject any characterisation of the cyber domain as 'subject to a discrete body of law'.[17] Consequently, as Knut Dormann concludes, the fact that a particular military activity is not specifically regulated does not mean that it can be used without extant restrictions.[18]

Strategic Implications & The Cardinal Principles of LOAC

Perhaps a close examination of some of the 'cardinal' principles of LOAC may provide some further guidance regarding the use of cyber weapons in armed conflict. Take, for example, the principle of distinction. Analysts and experts argue that there are not many conventional weapons that can be regarded as those 'incapable of distinguishing between civilians and military targets'.[19] This opinion was reflected in the commentary regarding the use of nuclear weapons where Judge Higgins called such weapons that were unable to distinguish between civilian and military targets 'blind' because of their nature.[20] It can be inferred from those analyses that some weapons may be confused as being a 'blind' weapon, but only because of a conscious decision to not directly attack military targets.

An analogy can be drawn between other 'blind' weapons, such as biological attacks that are unable to distinguish between military targets and civilians, and the debate around cyber weapons. In the case of biological weapons, a biological virus indiscriminately attacks from both military and civilian hosts. In a cyber context, a computer virus may spread from a military computer to civilian networks, causing significant loss of life. This may just be a hypothetical scenario, but it raises significant issues concerning strategic decisions about which weaponry to employ and the appropriate State response.

The principle of distinction also brings strategic consequences to consider in the cyber context, and not just IHL considerations. The features of the new cyber domain, such as interconnectivity, bring significant utility to States and society in peacetime. However, in times of armed conflict the ability to prevent significant collateral damage to the civilian population may be hampered by the interconnectedness of military networks and their dependence on civilian cyber infrastructure.[21] Indeed, States recognise the strategic importance of such critical infrastructures to national survival today, just as they did almost a century ago.[22] In terms of military necessity and proportionality, the interconnectedness of these systems only increases the risk of 'knock on' effects that cause loss of life or significant humanitarian consequences for the civilian population.[23] [24] During the 1990-91 Gulf War an attack on the Iraqi electric grid successfully disrupted military command and control networks. The attack also denied electricity to the civilian population, thereby affecting hospitals, emergency response, etc.[25] Although this example was a result of a kinetic military operation, the intended effect of a cyber operation may also have similar unintended consequences for the civilian population.

The Stuxnet Worm is a clear example of the challenges presented by the 'new method of warfare', particularly with regard to *jus ad bellum* and attributing armed attacks to a State. Ralph Langer, a German computer security expert, argues that the Stuxnet virus was only possible for an organisation that had State resources to support the attack.[26] In an interview, Langer added that Stuxnet was aimed at 'destroying its targets with utmost determination

in military style' and was widely believed to have been aimed at Iran's nuclear enrichment program.[27] Even though it is widely believe that critical infrastructure was the target, no State has claimed responsibility for the attacks and computer forensics have not conclusively attributed the virus to any State.[28] In the Tallinn Manual, Rule 7 states 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.'[29] This raises significant questions concerning States, who are victim to a cyber attack, and their right of self-defence.[30]

The above example also does not fit 'neatly' into the principles of military necessity and proportionality. Even if attribution to a belligerent state is achieved, the fundamental principles of LOAC may prevent a cyber response from the victim state. International law researcher Heather Dinniss argues that armed force in self-defence is only legitimate if it used to repel an attack, and other non-forcible remedies have proven unsatisfactory.[31] Moreover any response taken under the principle of military necessity should be made without undue delay.[32] In the cyber warfare context this raises questions as to the timeliness of a response to a cyber attack. Consider international law professor, Nicholas Tsagourias' assessment: 'Three characteristics of cyberspace make attribution extremely difficult… "anonymity"… multi-stage cyber attacks… operated by different people and placed in different jurisdictions… and the third is the speed with which a cyber attack can materialise'.[33] Even though States may be able to identify where a cyber attack originated from, the time delay in which the attacker is identified means that an armed response in self-defence (with military necessity considerations) may not be legally justified.

Potential strategic gains from cyber warfare, and associated methods, may exist even if they directly contravene IHL and LOAC principles. In 2002, Michael Schmitt suggested that the application for IHL should consider a consequence-based approach rather than applying the international law to specific States or actors.[34] This is because not all cyber methods, however, fall under the threshold of an 'armed attack'.[35] Consider, for example, a NATO bombing strike against a state-owned television network being used as a military communications hub, but the majority of its time is spent as a workplace for civilians not contributing to the conflict. An airstrike would knock out that communications network, but also cause significant civilian casualties. The targeting of civilians, other protected persons or objects with armed force is unlawful regardless of the means employed. In this scenario, however, a cyber weapon may be used to achieve the same effect whilst avoiding condemnation over striking a civilian target.[36] This then becomes a debate over military ethics rather than the application of international law, but this does raise questions regarding the use of cyber weapons to achieve similar effects to kinetic weapons, without civilian casualties.

Toward a Cyber Treaty?

What may be appropriate to protect civilians is an overarching international treaty regulating the use of cyber weapons in all scenarios. Existing international laws support coercive measures (though not armed attacks) to use against economic wrongs and violations of arms control treaties by States. Thus, these rules may also apply to using cyber weapons for those ends.[37] In the economic domain, State responses to violations are known as 'countermeasures' and in the arms control domain they are called 'sanctions'.[38] Both methods, as Mary O'Connell suggests, are coercive methods of enforcement that do not involve significant military force and can still achieve the aim of responding to a wrongful act.[39] This is a particularly important consideration, given numerous arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, currently exist to address a how specific type of weaponry may or may not used in both armed conflict and peacetime.[40] The implications of having a cyber-specific treaty could serve, not only to clarify how cyber weapons may be employed, but also to protect the cyber domain for all States to maintain its viability for economic and communications uses.

Not everyone in the international law community, however, supports the view that a distinct cyber treaty is required. Jeffrey Kelsey, in his *juris doctor* thesis, argues that treaties are not the answer; norms regarding the use of cyber weapons should evolve through custom, codes of conduct, or rules of engagement.[41] Kelsey suggests this method as the most efficient means of contributing to IHL, as 'any action toward a new treaty would be premature'.[42] Similarly, United States Military lawyer Bryan Ellis suggests this is because states will actively 'avoid prematurely limiting a weapon that could potentially offer some measure of non-lethality to conflict'.[43] Furthermore, Ellis submits that whilst a ban or treaty would be logical, its application may be unrealistic. There are two reasons for this

argument. Firstly, many cyber capabilities are dual-use and have peaceful utility for civilians.[44] Secondly, a treaty may regulate States' behaviour but not necessarily prevent non-state actors from breaching the principles of the treaty. This is because smaller States may seek to enhance their cyber capabilities as a force multiplier against more powerful opponents.

Perhaps another barrier to further development of binding laws on cyber warfare is the fact that the full effect of cyber weapons have not been seen. 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 restrict cyber weaponry. Consider Professor Robin Geib's assessment of why it would be difficult to find agreement regarding an international cyber weapons treaty:

'Visible or readily discernable 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—e.g. the manipulation of a nuclear power plant via cyberspace—really are'. [45]

Thus gains to understanding IHL may be made through encouraging internationally accepted norms, as Kelsey and Ellis suggest, rather than trying to enforce an international treaty. Indeed, the experts agreed to this consideration when drafting the Tallinn Manual.[46]

Future Considerations

Perhaps a cyber attack that shocks the consciousness of humanity could provide some insight on how to regulate cyber weapons for IHL. Unlike the nuclear proliferation debate, there are no clear examples of the extent of the damage possible through cyber weapons. Analysts and theorists can only debate worst-case scenarios and try to assess likely courses of actions by States. Moreover, the strategic implications of the advanced technology may be an incentive for States to not agree to regulation, particularly due to its utility in international disputes short of armed conflict. This is certainly one of the limitations of the Tallinn Manual in that it fails to address, but acknowledges this limitation, other scenarios short of armed conflict and how existing international laws may apply.

This means that significant debate is required over the scope of cyber capabilities and how they might be used in future armed conflicts and in international relations. It behooves States to consider the impact of this 'new form of warfare' on civilians. Not just from a legal and strategic perspective, but also because of the ethical implications of employing these mechanisms against civilians, protected persons and objects. It may be that cyber weapons and capabilities become more prominent in resolving international disputes due to their ability to achieve the same effects as kinetic weapons but without the associated damage to objects or civilian casualties. Even though the short-term effects may be irritable to the 'victim' State, these effects may be preferred over the long-term effects of civilian deaths and physical destruction to property.

Conclusion

The quote at the beginning of this paper neatly summarises the Tallinn Manual on the International Law Applicable to Cyber Warfare and its implications for international humanitarian law. The main conclusion of the Manual is that the cyber domain is not distinct and that extant laws do apply to cyber means in armed attacks. The Manual, however, only provides interpretations of how these laws are applied in cases of armed conflict and does not address issues below this threshold. This raises significant legal, ethical and strategic questions to consider when determining the future application of cyber weapons. Even the 'cardinal principles' do not provide a definitive answer as to how and when cyber weapons may be used in self-defence, for example. It is clear from the literature that there is no consensus as to the way forward in terms of regulating cyber weapons for IHL concerns; there are arguments in favour of international treaties and there are analysts who support the idea of international norms to regulate the use of cyber weapons in armed attacks. Future documents will need to address both sides. The aim, however, must focus on the protection of civilians and not the military advantages that cyber weaponry can provide States during armed conflict. Otherwise the world may see a cyber attack that truly shocks the conscience of humanity if not

properly regulated.

Bibliography

BBC, 'NATO Denies Targeting Water Supplies', BBC World Online Network, 24 May 1999, accessed 03 October 2013, <http://www.news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm>.

Betz, D.J. and Stevens, T., *Cyberspace and the State: Toward a Strategy for Cyber-Power,* International Institute of Strategic Studies, Routledge, London, November 2011.

Blake, D. and Imburgia, J.S., 'Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons"', *Air Force Law Review,* Vol. 66, 2011, pp. 157-203.

Department of Defence, 'Basic Principles of the Law of Armed Conflict', *ADDP 06.4—Law of Armed Conflict,* Department of Defence, Canberra, 2006, Chapter 2.

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

Dinstein, Y., 'The Principle of Distinction and Cyber War in International Armed Conflicts',*Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, p. 261-277.

Ellis, B.W., 'The International Legal Implications and limitations of Information Warfare: What Are Our Options?', Strategy Research Paper, US Army War College, 2001.

Fildes, J., 'Stuxnet Work "Targeted high-value Iranian Assets"', *BBC News,* 23 September 2010, accessed 30 September 2013, <http://www.bbc.co.uk/news/technology-11388018>

Fleck, D., '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, pp. 331-351.

Geib, R., 'The Conduct of Hostilities in and via Cyberspace', War and Law in Cyberspace Panel,*American Law in Society Proceedings*, 2010, p. 371-374.

Hilder, J., 'Computer Virus Used to Sabotage Iran's Nuclear Plan "Built by US and Israel"', *The Australian,* 27 January 2011.

International Committee of the Red Cross, 'Protocol Additional to the Geneva Conventions of 12 August1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun 1977', accessed 20 September 13, <http://www.icrc.org/ihl/WebART/470-750045?OpenDocument>

International Court of Justice, 'Dissenting Opinion of Judge Higgins', Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996, accessed 20 September 2013, <http://www.icj-cij.org/docket/files/95/7525.pdf>

Kelsey, J.T.G., 'Hacking Into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', *Michigan Law Review,* Vol. 106, 2008, pp. 1427-1451.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'The Tallinn Manual', accessed 12 Sep 13, <http://www.ccdcoe.org/249.html>

O'Connell, M.E., 'Cyber Security without Cyber War', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, pp. 187-209.

Prescott, J., 'War by Analogy', *The RUSI Journal,* Vol. 156, No. 6, December 2012, pp. 32-39.

Schaap, A.J., 'Cyber Warfare Operations: Development and Use Under International Law', *Air Force Law Review,* Vol. 64, 2009, pp. 121-173.

Schmitt, M.N., 'Wired Warfare: Computer Network Attack and Jus In Bello', *International Review of the Red Cross,* Vol. 84, No. 846, 2002, p. 365-399.

Schmitt, M.N., 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal,* Vol. 54, December 2012, pp. 13-37.

Schmitt, M.N., 'Classification of Cyber Conflict', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, pp. 245-260.

Schmitt, M.N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* , Cambridge University Press, 2013, <http://www.ccdcoe.org/249.html>

Sherry, M.S., *The Rise of American Air Power,* Yale University Press, New Haven, 1987.

Solis, G., *The Law of Armed Conflict: International Humanitarian Law in War,* Cambridge University Press, New York, 2010, p. 22.

The White House, *National Strategy to Secure Cyberspace,* Washington DC, 2003, p. vii, <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>

Tsagourias, N., 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, p. 229-244.

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

[1] This is actually misattributed to Keynes after his death. The original quote comes from Carvath Read,*Logic: Deductive and Inductive,* (1st ed. 1898), p. 351, eBook accessed 21 September 2013, < http://www.gutenberg.org/files/18440/18440-h/18440-h.htm#Page_351>

[2] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 'The Tallinn Manual', accessed 12 Sep 13, <http://www.ccdcoe.org/249.html>

[3] *Jus ad bellum* refers to the rules and laws that govern the lawfulness of the resort to armed conflict, whereas*jus in bello* concerns the rules and laws governing the conduct of armed conflict. Adapted from G. Solis,*The Law of Armed Conflict: International Humanitarian Law in War,* Cambridge University Press, New York, 2010, p. 22.

[4] M.N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber*

Warfare, Cambridge University Press, 2013, <http://www.ccdcoe.org/249.html>

[5] The Principles of LOAC: military necessity, avoidance of unnecessary suffering, proportionality, and distinction. From Department of Defence, 'Basic Principles of the Law of Armed Conflict', *ADDP 06.4—Law of Armed Conflict,* Department of Defence, Canberra, 2006, Chapter 2.

[6] 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, pp. 332-335.

[7] Ibid., pp. 349-351.

[8] M.N. Schmitt, 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal,* Vol. 54, December 2012, pp. 13-37.

[9] Ibid., p. 17.

[10] Ibid.

[11] Fleck, op. cit., p. 337.

[12] M.E. O'Connell, 'Cyber Security without Cyber War', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, pp. 192-193.

[13] Schmitt, 'International Law in Cyberspace', p. 19.

[14] The International Group of Experts defined the 'means of cyber warfare' as cyber weapons and their association cyber systems. The 'methods' are considered the techniques and procedures associated with the means in order to conduct a cyber attack. However, there is no complete list of 'cyber weapons'. Thus, according to the experts, cyber means of warfare include any cyber decide, instrument, mechanism, equipment or software used in a cyber attack. Adapted from *Tallinn Manua*l, pp. 141-142.

[15] Schmitt, 'International Law in Cyberspace', p. 17.

[16] AP 1 states: *In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.* From International Committee of the Red Cross, 'Protocol Additional to the Geneva Conventions of 12 August1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 Jun 1977', accessed 20 September 13, < http://www.icrc.org/ihl/WebART/470-750045?OpenDocument>

[17] Schmitt, op. cit.

[18] K. Dormann, 'Applicability of the Additional Protocols to Computer Network Attacks', Conference Paper delivered at the International Expert Conference on Computer Network Attacks and Applicability of International Humanitarian Law, 19 November 2004, accessed 30 September 2013, < http://www.icrc.org/eng/resources/documents/misc/68lg92.htm>

[19] 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.

[20] International Court of Justice, 'Dissenting Opinion of Judge Higgins', Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), 1996, accessed 20 September 2013, <http://www.icj-cij.org/docket/files/95/7525.pdf>

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

[22] An analogy can be drawn between security analysts' fear of the onset of airpower and recent debate regarding cyber warfare. Consider the language of Basil Liddell-Hart: *'a nation's nerve system, no longer covered by the flesh of its troops is now laid bare to attack, and, like the human nerves, the progress of civilization has rendered it far more sensitive than in earlier and more primitive times.'* Compare the similarities between Liddell-Hart's analysis to US National Cyber Strategy in 2003: *'Cyberspace is their (our nation's critical infrastructures) nervous system – the control system of our country.* Both statements signify awareness of new technology and its impact to strategic considerations. Even though there is no specific mention of IHL, these statements provide considerations on the 'new method' of warfare's impact on civilians. See M.S. Sherry, *The Rise of American Air Power,* Yale University Press,

New Haven, 1987, p. 36 and The White House, *National Strategy to Secure Cyberspace,* Washington DC, 2003, p. vii, <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>

[23] The Australian Defence Force defines the principle of 'military necessity' to allow States to use measures, not forbidden by international law to accomplish a legitimate military objective. The ADF Manual on LOAC also emphasises the notion that military necessary should aim to secure submission of the opponent at the 'soonest moment'. The principle of 'proportionality' requires that the losses and damage resulting from military action should be proportion in relation to the anticipated military advantage. From Department of Defence, 'Law of Armed Conflict', paras 2.1-2.8.

[24] M.N. Schmitt, 'Wired Warfare: Computer Network Attack and Jus In Bello', *International Review of the Red Cross,* Vol. 84, No. 846, 2002, p. 392.

[25] *Ibid.* For a similar situation see BBC, 'NATO Denies Targeting Water Supplies', BBC World Online Network, 24 May 1999, accessed 03 October 2013 <http://www.news.bbc.co.uk/hi/english/world/europe/newsid_351000/351780.stm>. In this situation a NATO air strike targeted Yugoslavia's electrical supply network during 'Operation Allied Force', one consequence of that attack resulted in the shutdown of pumping stations, disrupting the supply of fresh water to civilians.

[26] J. Fildes, 'Stuxnet Work "Targeted high-value Iranian Assets"', *BBC News,* 23 September 2010, accessed 30 September 2013, <http://www.bbc.co.uk/news/technology-11388018>

[27] J. Hilder, 'Computer Virus Used to Sabotage Iran's Nuclear Plan "Built by US and Israel"', *The Australian,* 27 January 2011.

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

[29] Tallinn Manual, 'Rule 7', pp. 34-35.

[30] See Art. 51 of the UN Charter, <http://www.un.org/en/documents/charter/chapter7.shtml>

[31] Dinniss, op. cit., p. 102.

[32] Y. Dinstein, *War, Aggression and Self-Defense*, (3rd ed.), Cambridge University Press, New York, 2001, p. 210.

[33] N. Tsagourias, 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law,* Vol. 17, No. 2, 2012, p. 233.

[34] Schmitt, 'Wired Warfare', pp. 374-375.

[35] Ibid.

[36] This scenario was adapted from an actual NATO airstrike against Serbian State Television in April 1999. See Schmitt, 'Wired Warfare', pp. 381-382.

[37] O'Connell, 'Cyber Security without Cyber War', p. 203.

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

[39] O'Connell, op. cit.

[40] Ibid., p 205.

[41] 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. 1449-1450.

[42] Ibid.

[43] B.W. Ellis, 'The International Legal Implications and limitations of Information Warfare: What Are Our Options?', Strategy Research Paper, US Army War College, 2001, p. 14.

[44] Ibid.

[45] Geib, 'The Conduct of Hostilities', p. 372.

[46] The Tallinn Manual, p. 5.

—-

Written by: Nam Nguyen
Written at: Australian Defence Force Academy / University of New South Wales
Written for: Dr Gavin Mount
Date written: November 2013