THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE: A BRIEF INTRODUCTION ON ITS TREATMENT OF *JUS AD BELLUM* NORMS

Myrna Azzopardi*

1. Introduction

The Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter the 'Tallinn Manual')[1] was an ambitious project taken on by a group of experts brought together at the initiative of the North Atlantic Treaty Organisation (hereinafter 'NATO') Cooperative Cyber Defence Centre of Excellence based in Tallinn, Estonia. It commenced in 2009 and, after three years, the International Group of Experts (hereinafter 'the Experts') produced a manual on the law governing cyber warfare.

Estonia was the victim of much publicised cyber attacks in 2007, which have energised the ongoing legal debate on the nature of cyber warfare, especially between States. The cyber attacks started after a dispute arose over the removal of a war memorial in Tallinn which angered ethnic Russians living there. Estonia is one of the most wired countries in the world and, therefore, it was a prime target for the wave of Distributed Denial of Service attacks (hereinafter 'DDoS') which took place. Such attacks essentially overload sites with traffic so that users may not access them. Over the course of three weeks, different sites ranging from those of news outlets to banks were jammed. It was claimed that some of the attacks could be traced back to Russia, even from State authorities, although Russia has always denied involvement.[2]

The approach the Experts took is important to note in order to understand the entire rationale behind the Tallinn Manual. In the words of Michael Schmitt[3] in his address at CyCon 2012, 'there is no effort to progressively develop the law' and the Tallinn Manual

* Myrna Azzopardi is currently reading for a Doctor of Laws degree at the Faculty of Laws, University of Malta. She has recently completed a course on International Security and Intelligence at Pembroke College, University of Cambridge, with a particular focus on cyber warfare.

[1] Michael N Schmitt (ed), Tallinn Manual on the International Law Applicable to Cyber Warfare (CUP 2013), electronic text available from Cambridge University Press and at <http://www.ccdcoe.org/249.html> accessed 13 July 2013.

[2] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia' (*The Guardian*, 17 May 2007) <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> accessed 14 July 2013.

[3] Michael Schmitt is one of the foremost writers on the subject of cyber warfare. He is the general editor of the Tallinn Manual and between 2009 and 2012 he served as Director of the NATO Cooperative Cyber Defence Centre of Excellence's Tallinn Manual project. Among his most noted works, there are 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999) 37 Columbia Journal of Transnational Law 885, and 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 Villanova Law Review 569.

is an application of accepted norms in international law.[4] It is an exercise in *lex lata,* not *lex ferenda* i.e. an exercise in the law which currently exists and not an attempt to create law*.* The Experts drew from several established treaties and judgments, among them the Geneva and Hague Conventions and the *Nicaragua* judgment. Consequently, there are few Rules in the Tallinn Manual which do not have an exact analogous provision in a Treaty elsewhere or are not reflected in customary international law.[5] This firmly places the Tallinn Manual within the school that believes that established international law may be applied to cyber warfare.

Throughout the Tallinn Manual (as noted by the Experts in the Commentaries to each of the Rules) the challenges arising from the apt application of established international law principles to the realm of cyber warfare are never lacking, none more so than the crucial question of defining 'attacks' within the cyber context. The Tallinn Manual is particularly concerned with *jus in bello* (the law of armed conflict or international humanitarian law) and *jus ad bellum* (the set of rules to be consulted before engaging in war) and does not deal with cyber crime[6] in general or cyber terrorism. It also treats cyber espionage which is an increasing concern to many States, most notably between the United and China.[7] This legal update focuses on the rules set out for *jus ad bellum.* The Tallinn Manual deals with attacks between cyber platforms, even if repercussions are felt in the physical world. It does not, for example, treat a mission which sets out to bomb a physical cyber control centre. That would fall within the realm of conventional warfare whose target simply happens to be a centre devoted to cyber infrastructure, in the same way that it could have been any other military building. Instead the Experts considered how established international law principles may be extended to the treatment of warfare by cyber means in the same way as had been done with the invention of nuclear weapons. For example, the rule that 'civilians and non-combatants remain under the protection and authority of the principles of international law'[8] has been incorporated within the Tallinn Manual.

[4] US Naval War College 'CyCon 2012: Michael Schmitt - Tallinn Manual Part 1' (29 September 2012) <http://www.youtube.com/watch?v=wY3uEo-Itso> accessed 9 February 2013.

[5] Each Rule is accompanied with a commentary that expounds on its legal basis and even tackles differences in interpretation.

[6] This falls within the remit of Council of Europe, Convention on Cybercrime, Budapest (23 November 2001) <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> accessed 16 March 2013.

[7] Danny Yadron and Siobham Gorman, 'U.S., Firms Draw a Bead on Chinese Cyberspies' (*Wall Street Journal*, 12 July 2013) <http://online.wsj.com/article/SB10001424127887324694904578600041603746114.html> accessed 14 July 2013.

[8] 1977 Additional Protocol to the 1949 Geneva Conventions - Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), art 1(2), 8 June 1977, 1125 U.N.T.S. 3. This is reflected in Tallinn Manual (n 1) Rule 32.

Schmitt notes that 'it has been well accepted that a lack of directly applicable treaty law does not create an international humanitarian law-free zone'[9] and, furthermore, that 'the Experts rejected any characteri[s]ation of cyberspace as a distinct domain subject to a discrete body of law'[10] as the 'application of international law to cyber activities is accordingly a matter of identifying the relevant legal principles that bear on the person, place, object, or type of activity in question.'[11]

2. Sovereignty and Jurisdiction

The point of departure is that no single State has jurisdiction over cyberspace as a whole. Therefore, the Tallinn Manual begins with: 'A State may exercise control over cyber infrastructure and activities within its sovereign territory.'[12] Sovereignty over cyber infrastructure may be exercised regardless of whether it is Government or privately owned.[13] The fact that any given cyber infrastructure is part of a more global network does not imply a waiver of a State's sovereignty.[14] The territorial limit also includes the seabed of the territorial sea, important to note because submarine cables often carry international internet communications.[15] The exercise of sovereign rights is especially poignant when considering shut downs to the access of the Internet, as has been happening in the Syrian conflict for the last two years.[16] The legitimacy of this often comes into question. A State has the right to do this, provided it complies with international human rights and telecommunications law.[17]

A State may exercise its jurisdiction:

(a) Over persons engaged in cyber activities in its territory;
(b) Over cyber infrastructure located in its territory; and
(c) Extraterritorially, in accordance with international law.[18]

Under the above Rules, the exercise of jurisdiction afforded by the Tallinn Manual is on several bases including Subjective Jurisdiction, when the cyber operation has been initiated within a State's territory, irrespective of where the effects occur; and Objective Jurisdiction, when the effects of cyber operations initiated outside a State's territory are

[9] Michael Schmitt 'International Law in Cyberspace: The Koh Speech and *Tallinn Manual* Juxtaposed' (2012) 54 Harvard International Law Journal 13, 17.
[10] ibid.
[11] ibid.
[12] Tallinn Manual (n 1) Rule 1.
[13] ibid Rule 1 comment (hereinafter 'cmt') 5.
[14] ibid Rule 1 cmt 10.
[15] ibid Rule 1 cmt 11.
[16] Martin Chulov, 'Syria Shuts Off Internet Access Across the Country' (*The Guardian*, 29 November 2012) <http://www.guardian.co.uk/world/2012/nov/29/syria-blocks-internet> accessed 9 February 2013.
[17] Tallinn Manual (n 1) Rule 1 cmt 10.
[18] ibid Rule 2.

felt within it, as happened in the Estonia attacks.[19] These attacks had grave effects such as the interference with banking systems and governmental functions.[20] The Experts also noted that other theories of jurisdiction may also be adopted including the Active Personality Principle (due to the nationality of the perpetrator); the Passive Personality Principle (due to the nationality of the victim); and, most relevant, the Protective Principle (on the basis of national security).[21] The possible application of all the above principles does signify that multiple States may enjoy jurisdiction over a particular cyber incident,[22] especially in light of mobile-computing devices and cloud-based services. It is important, however, that actual physical presence is established.[23]

The requirement for physical presence raises the point of the inherent difficulty in determining jurisdiction due to such techniques as hiding Internet Protocol (IP) addresses. The complex and international nature of network infrastructures does not, in its very nature, co-operate with the traditional notions of territorial sovereignty. However, some certainty may be derived from the above rules so as not to deny a State the right to exercise sovereignty where it is clear that it may do so.[24] Furthermore, a State's cyber infrastructure is granted sovereign immunity if devoted solely to Government purposes,[25] in much the same way that ships owned by the State enjoy this immunity. By way of example, a denial of service attack against a State's military satellite would be a violation of sovereign immunity.

3. State Responsibility and Attribution

Rule 6 of the Tallinn Manual lays out that a State shall bear international legal responsibility for a cyber operation attributable to it. This is based on customary international law and reflected in the International Law Commission's Articles on State Responsibility.[26] The matter is quite straightforward when concerned with State organs that, even if acting beyond their instructions but still officially, shall be attributable to the State.[27]

The notion of attribution becomes complex when considering non-State actors. For the purposes of this Rule, persons or entities authorised by the State shall be equated to

[19] ibid Rule 1 cmt 6.
[20] ibid Rule 2 cmt 7.
[21] ibid Rule 1 cmt 8.
[22] ibid Rule 1 cmt 9.
[23] ibid Rule 2 cmt 5.
[24] ibid Rule 2 cmt 3.
[25] ibid Rule 4: 'Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.'
[26] International Law Commission, Responsibility of States for Internationally Wrongful Acts, GA Res. 56/83 annex, UN Doc. A/RES/56/83 (12 December 2001).
[27] Tallinn Manual (n 1) Rule 6 cmt 7.

State organs, for example Emergency Response Teams authorised to defend government cyber infrastructure and networks.[28] Consider the example where a State employs private citizens to carry out its work; whereby under Article 8 of the Article on State Responsibility, the State shall be held responsible because the private entity is 'acting on the instructions' of the State.[29] The Experts made reference to two prolific judgments on the matter which sets out relevant tests.[30] The first is the 'effective control' test described by the International Court of Justice (hereinafter 'ICJ').[31] This test holds that a State is only responsible for the actions of non-State actors if the actors are in 'complete dependence' of the State. In the *Nicaragua* judgment, which sets out this test, although the US had financed and organised the rebels fighting the Nicaraguan Government, it did not have 'effective control' over the operations in which the violations were committed.[32]

The second is the 'overall control' test introduced by the International Criminal Tribunal for the Former Yugoslavia (hereinafter 'ICTY') in the *Tadić* case, which is a less stringent test.[33] The 'overall control' test would need to be beyond 'the mere financing and equipping of such forces and involv[e] also participation in the planning and supervision of military operations.'[34] The State 'needs to have issued specific instructions or directed or controlled a particular operation […] Merely encouraging or otherwise expressing support for the independent acts of non-State actors does not meet the […] threshold.'[35] However, if the tools provided by one State land in the hands of insurgents acting against another State but under no instruction from the first State, then the latter should not be held responsible.[36] Furthermore, there was the significant contribution made by the *Tehran Hostages* case[37] which adopts Article 11 of the Articles

[28] ibid Rule 6 cmt 8.

[29] (n 26) art 8.

[30] For an interesting comparison of these tests in their application to cyber warfare, see Marco Roscini, 'World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law; Scott J Shackleford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2nd International Conference on Cyber Conflict, Tallinn, June 2010).

[31] *Nicaragua* judgment, Military and Paramilitary Activities in and Against Nicaragua (*Nicaragua v US),* 1986 ICJ 14 (June 27) [115].

[32] Tallinn Manual (n 1) Rule 6 cmt 10.

[33] *Prosecutor v Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment (ICTY, 15 July 1999). This test, in its origin, operated within the remit of ICTY to determine individual criminal responsibility, different to that of the ICJ. Therefore, the Experts are here proposing it as an alternative threshold to establish State attribution, irrespective of individual responsibility.

[34] ibid [145].

[35] Tallinn Manual (n 1) Rule 6 cmt 11.

[36] ibid Rule 6 cmt 13.

[37] United States Diplomatic and Consular Staff in Tehran (*US v Iran),* 1980 ICJ 3 (May 24).

on State Responsibility, where acts are attributable if 'the State acknowledges and adopts the conduct in question as its own'.[38]

As a final corollary, simply because a cyber operation originates from a Governmental infrastructure does not automatically signify that the State should be held responsible.[39] Furthermore, '[t]he fact that a cyber operation has been routed via the cyber infrastructure located in a State is not sufficient evidence for attributing the operation to that State.'[40]

4. Re-Imagining the Concept of 'Use of Force'

The ICJ has stated that the prohibition on use of force and the right to self-defence applies 'regardless of the weapons employed.'[41] Therefore, uses of force by cyber means may too be prohibited. Rule 10 of the Tallinn Manual reads: '[a] cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.'[42]

The above rule is a reflection of a promulgated customary international norm. The Tallinn Manual suggests a definition of 'use of force' in cyberspace based on the effects–based threshold: 'A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.'[43] Here we have one of the most crucial complexities of applying established norms to the realm of cyber warfare. Based on previous agreements at an international level, the Experts concluded that economic coercion does not constitute a use of force.[44]

To treat the remaining scenarios where actions fall short of use of force, the Experts identified eight key factors:[45]

[38] Tallinn Manual (n 1) Rule 6 cmt 14: "Note that this provision is narrowly applied. Not only are the conditions of 'acknowledgement' and 'adoption' cumulative, they also require more than mere endorsement or tacit approval."

[39] ibid Rule 7.

[40] ibid Rule 8.

[41] *Nuclear Weapons Advisory Opinion*, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 ICJ 226 (July 8) [39].

[42] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, art 2: 'All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.'

[43] Tallinn Manual (n 1) Rule 11. The wording of this Rule was drawn from the *Nicaragua* judgment.

[44] ibid Rule 11 cmt 2.

[45] ibid Rule 11 cmt 9. Jason Barkham has been particularly critical of these criteria. See 'Information Warfare and International Law on the Use of Force' (2001) 34 NYU Journal of International Law 57.

1. Severity

A cyber operation that results in 'damage, destruction, injury, or death' will be considered as a use of force but acts which generate 'mere inconvenience or irritation' will not be considered as such.

2. Immediacy

A State is more likely to categorise an act as a use of force if the repercussions are felt quickly.

3. Directness

The causal relationship between a cyber operation and its consequences must be manifest. The Experts, here, say that the effects of economic sanctions, for example, take long to be felt and might not easily be deemed uses of force.

4. Invasiveness

The degree to which a cyber operation intrudes into targeted systems is critical to exclude attacks which would not fall under the regime of cyber warfare, such as attacks aimed at non-State agencies, which have no great impact on the State.

5. Measurability of the effects

Technological consequences are difficult to quantify but if they may be expressed in real terms then it is more likely that they are deemed uses of force.

6. Military character of the cyber operation
7. Extent of State involvement
8. Presumptive legality

The Experts argue that, generally, in international law, acts that are not forbidden are permitted. This emanates from a decision taken by the Permanent Court of International Justice.[46]

5. Self-Defence

'A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.'[47]

The Tallinn Manual has adopted one of the three main approaches which scholars have used to treat the application of self-defence to armed attacks – the effects-based approach. The other two are the target-based approach and the instrument-based approach. The latter treats a cyber attack as an armed attack only if it uses military weapons. The target-based approach limits the application to internationally accepted targets, usually military or specifically State sponsored ones. The effects-based approach provides the most dynamic interpretation of the three, useful due to the lack of foreseeability of cyber warfare.

[46] *Lotus Case*, S.S. 'Lotus' (*France v Turkey*), 1927 PCIJ (ser. A) No. 10, (7 September).

[47] Tallinn Manual (n 1) Rule 13.

Importantly, the Experts note that 'the term 'armed attack' is not to be equated with the term 'use of force' appearing in Rule 11.'[48] The ICJ stated that not every use of force rises to the level of an armed attack[49] and only when it does reach that level is a State allowed to use force as self-defence. Essentially, the main criterion for categorising an attack as armed is that the act needs to be grave.[50] Therefore, some cases can easily be categorised as armed attacks, such as those which result in the injury of persons or property. The Experts agreed that acts of cyber intelligence gathering and brief interruption of non-essential cyber services do not rise to the level of armed attacks.[51]

The Experts themselves recognise the ambiguity of the definition given and felt it was unclear at which point death, injury, damage, destruction, or suffering caused by a cyber operation failed to qualify as an armed attack.[52] They did consider if a State were the subject of multiple cyber operations which cumulatively would have a destructive effect but would not alone qualify as armed attacks. Such is the likely risk of collective 'pinprick attacks'. In such cases, the determining factors are whether or not they were carried out with the same objective and whether, cumulatively, they satisfy the requisite scale and effects threshold.[53]

With regard to cases which fall short of injury, death or destruction but which are otherwise disturbing, the Experts, once again, could not reach a consensus, the prime example being a cyber attack on the New York Stock Exchange, causing the market to crash. Some Experts did not want to label it an 'armed attack' because it was a case of financial loss; others felt the effects would be too serious not to be considered as such.[54] This highlights the practical difficulties of eliminating economic repercussions as per conventional interpretations.

In determining whether a cyber attack is an armed attack or not, the Experts suggest the inclusion of the factor of foreseeability of the effects. By way of example, if a cyber operation targets a water purification plant, contamination of water and illness are foreseeable consequences.[55] The majority agreed that the original intention of the attack does not determine whether an operation is an armed attack or not. For example, an espionage operation which results in grave damage would still merit self-defence.[56] By extension, the Experts felt that a third party State is entitled to invoke self-defence if there are

[48] ibid Rule 13 cmt 5. Importantly, not all States accept this view.
[49] *Nicaragua* (n 31) [191] and [195].
[50] Tallinn Manual (n 1) Rule 13 cmt 5 and 6.
[51] ibid Rule 13 cmt 6.
[52] ibid Rule 13 cmt 7.
[53] ibid Rule 13 cmt 8.
[54] ibid Rule 13 cmt 9.
[55] ibid Rule 13 cmt 10.
[56] ibid Rule 13 cmt 11.

spill-over effects from attacks between two other States which reach the scale and effects criteria.[57] The object of the attack, however, does influence whether it is classified as an armed attack or not, so that damage to State property, for example, is more likely to be deemed an armed attack.[58] The question of non-State property would have to be determined on a case-by-case basis. All in all, the Experts felt that there has, as yet, been no attack which fulfils the criteria of an armed attack despite the popularly of the term 'cyber war'.

Once an operation is assessed to be an armed attack, self-defence may be exercised. Any self-defence undertaken must be necessary and proportionate[59] and the right to it arises if the attack is imminent.[60] If passive cyber defences, for example firewalls are sufficient then they must be used in lieu of other more aggressive measures.[61] Furthermore, defences need not necessarily be of the same nature. States may retaliate with cyber force to a kinetic attack and vice versa, so long as the criteria are met.[62]

'Immediacy' of the response, as a criterion, aims to distinguish 'an act of self-defence from mere retaliation'[63] and refers to the period immediately following the attack. The Experts offer the test of reasonableness to determine the period within which a response is to be initiated.[64]

Until arriving at a satisfactory assessment of the situation, the victim-State may use non-forceful measures and refer the matter to the Security Council.[65] Countermeasures are another alternative which the Tallinn Manual considers in Rule 9.[66] Countermeasures are responses to internationally wrongful acts in order to procure cessation and reparation.[67] The Experts agreed that if the act has ceased then countermeasures are not justified.[68] Countermeasures are distinct from actions on the

[57] ibid Rule 13 cmt 12.
[58] ibid Rule 13 cmt 18.
[59] ibid Rule 14; *Nicaragua* (n 31) [176], [194]; *Nuclear Weapons Advisory Opinion,* (n 41) [41].
[60] Tallinn Manual (n 1) Rule 15.
[61] ibid Rule 14 cmt 3.
[62] ibid Rule 14 cmt 5.
[63] ibid Rule 15 cmt 8.
[64] ibid Rule 15 cmt 9.
[65] ibid Rule 15 cmt 7; Rule 18 states:

> Should the United Nations Security Council determine that an act constitutes a threat to the peace, breach of the peace, or act of aggression, it may authori[s]e non forceful measures, including cyber operations. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures.

[66] 'A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.'
[67] Tallinn Manual (n 1) Rule 9 cmt 3.
[68] ibid.

basis of the 'plea of necessity',[69] whereby protective measures which violate the interests of other States may be invoked in exceptional circumstances. The Experts believe that it is under the plea of necessity where counter-hacking would be justified.[70] However, they note that the International Law Commission has stated that the 'plea of necessity' may be invoked when there are no other options available and this may not 'seriously impair essential interests of other States or those of the international community as a whole'.[71]

6. Conclusion

The Tallinn Manual is a welcome contribution to an area where very little consensus has been reached. It is an area which has, as yet, no clear delineation, where the terms 'cyber warfare', 'cyber terrorism' and 'cybercrime' are still often used interchangeably resulting in significant confusion. Some writers have scorned the application of international law to cyber warfare citing the very nature of the Internet[72] which cannot be based on traditional ideas of territorial jurisdiction. Others have even suggested that altogether new frameworks must be created to aptly deal with cyber warfare.[73]

Nevertheless, the Tallinn Manual will continue to generate discussion, not least of which because of some of its more controversial claims.[74] The United States has, most notably, acknowledged the growing concern of cyber warfare, going to so far as to set up the United States Cyber Command in 2009. It has admitted to orchestrating State-sponsored attacks, codenamed 'Olympic Games'[75] wherein Iran's nuclear program was deterred through the use of the Stuxnet worm, in 2009, and the Flame virus, in 2012. They adversely affected Iran's centrifuge machines which are used to enrich uranium and

[69] (n 26) art 25.
[70] Tallinn Manual (n 1) Rule 9 cmt 12.
[71] ibid Rule 9 cmt 10 and 12.
[72] Stewart A Baker and Charles J Dunlap Jr, 'What is the Role of Lawyers in Cyberwarfare?' (*ABA Journal*, 1 May 2012) <http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare> accessed 14 July 2013.
[73] Lawrence L Muir Jr, 'The Case Against an International Cyber Warfare Convention' <http://wakeforestlawreview.com/the-case-against-an-international-cyber-warfare-convention> accessed 9 February 2013.
[74] Dieter Fleck, 'Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual' [2013] J Conflict & Security Law <http://jcsl.oxfordjournals.org/content/early/2013/06/26/jcsl.krt011.abstract> accessed 9 July 2013.
[75] Reported by David E Sanger, the Chief White House correspondent for the New York Times in his 2012 book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Broadway 2012) For a preview, please see: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1&> accessed 9 February 2013.

collected valuable information.[76] Some of the experts were of the view that Stuxnet was the only case which reached the level of an armed attack.[77] As controversial as such a claim may be, it brings to light the new dimension of military operations.[78]

[76] Peter Beaumont and Nick Hopkins, 'US was 'key-player in cyber-attacks on Iran's nuclear cyber programme' (*The Guardian,* 1 June 2012) <http://www.guardian.co.uk/world/2012/jun/01/obama-sped-up-cyberattack-iran> accessed 9 February 2013.

[77] Tallinn Manual (n 1) Rule 13 cmt 13.

[78] Neil Ungerleider, 'Barack Obama is the First Cyber War President, but a President Can't Win A Cyber War' (*Fast Company*) <http://www.fastcompany.com/3005728/why-obama-first-cyberwar-president> accessed 14 July 2013.