Determining When Conduct in Cyberspace Constitutes Cyber Warfare in Terms of the International Law and *Tallinn Manual on the International Law Applicable to Cyber Warfare*: A Synopsis

Murdoch Watney(✉)

University of Johannesburg, Johannesburg, South Africa
mwatney@uj.ac.za

Abstract. Article 2(4) of the UN Charter provides that nation-states will refrain from the threat or use of force against the territorial integrity or political independence of any state. It is doubtful whether it will deter states from waging war in cyberspace. Cyber warfare is a perplexing and contentious issue within the ambit of international law. Discussions have focused on whether the existing rules and principles may be extended to cyberspace or whether new treaty law on cyber warfare must be drafted. Against this background the International Group of Experts drafted the Tallinn Manual on the International Law Applicable to Cyber Warfare at the invitation of the NATO Cooperative Cyber Defense Centre of Excellence. The Tallinn Manual provides rules in respect of cyber warfare. In the absence of a multilateral treaty it may be asked whether the Tallinn Manual will achieve acceptance on a global level as rules governing cyber warfare.

Keywords: Cyber warfare · Cyberspace · International law · Tallinn Manual · DDoS attacks on Estonia · Stuxnet attack on Iran · Armed attack

1 Introduction

On a national level nation-states are concerned about cyber threats and/or risks that may threaten their national cyber security and national critical information infrastructure. Not only on a national level, but also on an international level peace and security in cyberspace are an ongoing concern to ensure a safer and better cyber world for all.

There has been some debate on whether the existing rules and principles of the international law which were developed in a physical environment can be extended to the cyber environment or whether new treaty laws in respect of cyber warfare will have to be established.

This article is based on research supported in part by the National Research Foundation of South Africa (UID 85384). Opinions expressed are those of the author and not the NRF.

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2014
P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 130–143, 2014.
DOI: 10.1007/978-3-319-14289-0_10

It is therefore not surprising that the release in March 2013 of the Tallinn Manual on the International Law Applicable to Cyber Warfare (hereafter referred to as the Tallinn Manual) [1] have evoked some discussion. The Tallinn Manual is based on the application of the existing rules and principles of international law to cyberspace. In this paper the debate in determining when conduct in cyberspace amounts to cyber warfare will be specifically explored.

It is important to note that the Tallinn Manual is not the first to codify the application of international law in cyberspace. In January 2011 the EastWest Institute released the first joint Russian-American bilateral report "Working towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace" (hereafter referred to as the EWI Cyber Conflict Rules). [2] The EWI Cyber Conflict Rules is a Russia – US bilateral that focuses on the protection of critical infrastructure in cyberspace by means of international humanitarian law (IHL), also referred to as *jus in bello* (the law governing conduct in armed conflict and the treatment of combatants and civilians in time of armed conflict). The aim of the report was to explore how the humanitarian principles provided for in the Geneva and Hague Conventions on war may be extended to govern war in cyberspace [3].

For purposes of this discussion, the Tallinn Manual is applicable as its purpose is to identify the international law applicable to cyber warfare. It outlines for example the rules applicable to conduct that constitute cyber warfare.

The Tallinn Manual was drafted at the invitation of the North Atlantic Treaty Organisation Cooperative Cyber Defence Centre of Excellence (hereafter referred to as the NATO CCD CoE) under the directorship of Michael Schmitt, professor of international law at the United States Naval War College in Rhode Island. According to Schmitt: "We wrote it as an aid to legal advisers, to governments and militaries, almost a textbook. We wanted to create a product that would be useful to states to help them decide what their position is. We were not making recommendations, we did not define best practice, we did not want to get into policy" [3].

The main purpose of this paper is to investigate:

- When will conduct constitute cyber warfare in terms of the international law and the interpretation of the international law in accordance with the Tallinn Manual and other authors? The cyber attack in the form of a DDoS on Estonia and the attack by means of the Stuxnet worm on Iran will be evaluated in this regard.

  The following inter-related and overlapping aspects will also be referred to:
- As there are no treaty provisions that deal directly with 'cyber warfare', will the Tallinn Manuals' interpretation of international law in respect of cyber war be considered as a so-called textbook to all governments of not only western but also non-western nation states? This question is relevant as the author of this paper is from a non-western state and developing country, namely South Africa. Here cognizance should be taken of the controversy regarding the outcome of the World Conference on International Telecommunications (WCIT–12) held in 2012 by the International Telecommunications Union (ITU), which is a specialized agency of the United Nations.
- Although the Tallinn Manual [1] as well as the EWI Cyber Conflict Rules [2] make a valuable contribution to the better understanding of the application of international

law in cyberspace, would it not be better for the United Nations as a central body to conduct such a study involving the participation of all internet-connected nation-states?

2 Defining Concepts Relevant to the Discussion

There exists no universal definitions of the concepts relevant to the discussion but for purposes of this paper conceptualisation serves as a point of reference, despite the criticism that may be invariably leveled against the definitions.

It is proposed that the concept, 'cyber threat' or 'cyber risk' be used as an umbrella term which encompasses all threats to the interests of law enforcement and/or national security.

Cyber threats (risks) may be divided into cybercrime which will fall within the ambit of law enforcement investigations or so-called cyber-intelligence crimes such as cyber warfare, cyber terrorism or espionage which will fall within the ambit of national security. In the latter instance specific attention should be given to the protection of the critical infrastructure of a nation-state. The national critical information infrastructure includes all ICT systems and data bases, networks (including buildings, people, facilities and processes) that are fundamental to the effective operation of a nation-state [4]. The EWI Cyber Conflict Rules define critical infrastructure as those infrastructure whose continued operation is essential for sustaining life, economic stability and continuation of government that includes national security [2].

The Tallinn Manual paid particular attention to terminology [1]. It uses the term 'cyber operations' that is not derived from a legal term with a concrete meaning. 'Cyber operations' refers to the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyber space [1]. 'Cyber operations' includes cyber attacks as a specific category of cyber operations. 'Cyber attack' is defined in Rule 30 of the Tallinn Manual as 'a cyber operation whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects.' Non-violent attacks such as cyber espionage would in general not constitute a cyber attack.

The EWI Cyber Conflict Rules [2] states that there is no clear internationally agreed upon definition of what could constitutes 'cyber war'. For purposes of this paper 'cyber war' is defined as an action by a nation-state to penetrate another nation's computers and networks for purposes of causing damage or disruption. [5]. The Tallinn Manual state that there may be instances where the cyber operations by non-state actors will resort under 'cyber warfare.'

3 Cyber Warfare: Myth or Reality?

Prior to 2007 cyber attacks were nothing new. But 2007 saw the first reported cyber attack launched by means of distributed denial of service attacks (DDoS) against a nation-state namely Estonia. It was apparently the largest DDoS attacks ever seen [5]. The Estonian government estimates a million personal computers in a number of

different countries, including the US, Canada, Vietnam and Brazil were used to conduct the attack. The damage was thought to amount to tens of millions of Euros [6].

The cyber attack was allegedly caused by the removal of a statue of a Russian soldier, who had fought during the Second World War, from the main square in the capital city, Tallinn to a military cemetery. The removal of the statue was perceived by ethnic Russians living in Estonia and Russia as an affront to Russia and their sacrifices during World War II [5].

The Estonian cyber attack served as a wake-up call to the international community of the growing security threat of cyber attacks launched against a nation-state as well as the vulnerability of a nation-state regarding the protection of its national security which includes its critical infrastructure [6].

NATO took the cyber attack on Estonia seriously enough to result in the establishment of a NATO Co-operative Cyber Defence Centre of Excellence (CCD CoE) based in Talinn, Estonia. In October 2008 NATO's Northern Atlantic Council granted the NATO Co-operative Cyber Defence Centre of Excellence (NATO CCD CoE) full NATO accreditation and the status of an international military organisation. The NATO CCD CoE is a partnership between 11 states and the sponsoring nations are Estonia, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain and the US. In January 2013 David Cameron announced that the UK would be joining the CCD CoE in 2013 [7].

Whether the attack on Estonia amounted to an armed conflict will be discussed hereafter at paragraph 5. The attack however confirmed that any nation-state may become the victim of a cyber attack against its critical infrastructure, affecting national security.

Nation-states are currently implementing national cyber security framework policies to ensure the existence of a central body to oversee a legal framework to ensure a coordinated and aligned approach to cyber security issues that may affect the national cyber security of a nation state. Although such a coordinated and aligned approach on a national level may assist in the protection of its critical infrastructure, it is not infallible. If a national intelligence crime is committed against a state's critical infrastructure, the victim nation-state is confronted on an international level with the following questions:

- When will the conduct committed in cyberspace be defined by international law as armed conflict; and
- Which recourse does the victim nation-state have against the state responsible for the attack within the ambit of the international law?

Returning to 2009 and 2010 and possibly also 2008 when the worm, Stuxnet was created to cripple Iran's nuclear program by sabotaging industrial equipment used in uranium purification. Stuxnet targeted systems controlling high-speed centrifuges used in the Iranian nuclear programme to enrich uranium, causing them to slow down and speed up repeatedly until they failed under the abnormal mechanical strain. [8] The penetration technique of this 'cyber weapon' had never been seen before and was therefore what hackers call a 'zero-day attack', the first time use of a specific application that takes advantage of a hitherto unknown glitch in a software program [5]. The EWI Cyber Conflict Rules [2] refers to examples of cyber weapons used in cyberspace such as worms, viruses, remote manual control and key loggers.

The question focuses again on whether the conduct constitutes an example of cyber warfare [1]. What recourse did Iran have? These questions will be discussed at paragraph 5 hereafter.

In the EWI Cyber Conflict Rules [2] the following was stated regarding cyber warfare: '… there is considerable confusion. Senior government leaders from the same country have incompatible opinions about the most basic aspects of cyber war – its existence now, its reality or likely impact in the future. The current ambiguity is impeding policy development and clouding the application of existing Convention requirements.'

Against above-given background, NATO CCD CoE is of the opinion that cyber warfare is a reality and more than a mere myth otherwise it would not have invited the international law experts as far back as 2009 to draft a manual on the international law applicable to cyber warfare.

In 2010 NATO acknowledged this threat in its 2010 *Strategic Concept* wherein it committed itself to 'develop further our ability to prevent, detect, defend against and recover from cyber attacks including by using the NATO planning process to enhance and coordinate national cyber defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.' [1, 9].

Other nation-states have also indicated that they consider cyber warfare as a serious threat to national security which includes the critical infrastructure. In 2010 the UK's national security strategy characterised cyber-attacks, including those by other states, as one of four "tier one" threats alongside terrorism, military crises between states and major accident [8]. The US 2010 National Security Strategy likewise cited cyber threats as 'one of the most serious national security, public safety, and economic challenges we face as a nation' and in 2011 the US Department of Defense issued its *Strategy for Operating in Cyberspace* which designates cyberspace as an operational domain. In response to the threat the US has now established the US Cyber Command to conduct cyber operations. During the same time Canada launched *Canada's Cyber Security Strategy,* the UK issued the *UK Cyber Security Strategy Protecting and Promoting the UK in a Digitized World* and Russia published its cyber concept for the armed forces in *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space* [1, 9].

4 Scope and Application of the Tallinn Manual

The Tallinn Manual is a comprehensive legal manual that was drafted over a period of 3 years by 20 researchers which consisted of legal scholars and senior military lawyers (referred to as the International Group of Experts) from NATO countries. NATO consists of 28 independent member countries, consisting mostly of EU member countries as well as the US and Canada.

The Tallinn Manual is not on 'cyber security', but it specifically focuses on the application of international law in respect of cyber warfare which is one of the challenges facing nation-states. The International Group of Experts that drafted the Tallinn Manual was unanimously of the opinion that the general principles of international law

applies to cyberspace and that there is no need for new treaty law. The Tallinn Manual represents the International Group of Experts' interpretation of the international law in respect of cyber warfare.

The Tallinn Manual examines the international law governing

- *Jus ad bellum* (the law governing the right to the use of force by states as an instrument of their national policy) where it has to be determined in which circumstances cyber operations will amount to the use of force or armed attack justifying the use of necessary and proportionate force in self-defence or an act of aggression or threat to the international peace and security, subject to UN Security Council Intervention.
- *Jus in bello* (the international law regulating conduct in armed conflict; also referred to as the law of war or humanitarian law) with reference to armed conflict.

The Tallinn Manual's emphasis is on cyber-to-cyber operations such as the launch of a cyber operation against a states' critical infrastructure or a cyber attack targeting enemy command and control systems.

It is divided into 95 black-letter rules and accompanying commentary. The rules set forth the International Group of experts' conclusions as to the broad principles and specific norms that apply in cyberspace regarding cyber warfare. Each rule is the product of unanimity among the authors. The accompanying commentary indicates the legal basis, applicability in international and non-international armed conflicts and normative content of each rule. It also outlines differing or opposing positions among the experts as to the rules' scope or interpretation. The rules reflect the consensus among the International Group of Experts as to the applicable *lex lata,* the law that is currently governing cyber conflict. It does not set forth *lex forenda*, best practice or preferred policy.

Although the Tallinn Manual is not an official document that represents the views of the NATO CCD CoE or the Sponsoring Nations or NATO, Colonel Kirby Abbott (an assistant legal adviser at NATO) said at the launch of the Manual in March 2013 that the manual was now 'the most important document in the law of cyber warfare. It will be highly useful' [7].

It should be noted that NATO CCD CoE has launched a three year follow on project, 'Tallinn 2.0' that will expand the scope of the Tallinn Manual primarily in the law of State responsibility realm. 'Tallinn 2.0' will also be dealing with other bodies of so-called peacetime international law, as they relate to State responses, such as international telecommunications law, space law and human rights law [11].

5 Application of the International Law in Determining When Conduct Constitutes Cyber Warfare

5.1 International Law

International law does not apply the concept of 'act of war' in evaluating the legality of state violence, but international lawyers assess whether state actions constitute an

'illegal intervention', 'use of force', 'armed attack' or 'aggression.' This assessment involves

i. Interpreting these concepts in international law (doctrinal analysis); and
ii. Understanding how states react to events (evaluation of state practice).

International law as a matter of doctrine prohibits a state from intervening in the domestic affairs of other states, using force or the threat of force against another state or engaging in acts of aggression [12, 13].

Article 2(4) of the UN Charter states: 'All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state or in any other manner inconsistent with the Purposes of the United Nations.'

These rules establish thresholds that distinguish between

- Intervention from uses of force; and
- Uses of force from an armed attack.

Determining into which category state behaviour falls is not easily established. The International Court of Justice has ruled that not all types of force constitute armed attacks [10]. Only where the use of force is a serious use of force can the victim state react in self-defense and then the self-defense must comply with the proportionality requirement. Similarly some damaging covert actions are illegal intervention but not use of force.

A state can only legally use force if it is the victim of an armed attack or if the United Nations Security Council has authorized it.

Article 51 of the UN Charter states: 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.'

Determining which type of threshold an action crosses usually involves evaluating its effect or consequences on a case-by-case basis. The International Group of Experts also states that the effects and scale of the attacks are relevant in determining when the threshold of the attack will rise from unlawful intervention to illegal use of force to armed conflict. Fidler [12] refers to the following criteria to assess whether the incident constitutes an intervention, use of force or armed attack:

(a) Instrumentalities refer to the means or methods used;
(b) Effects refer to the damage to tangible objects or injury to humans;
(c) Gravity refers to the damage or injury's scale or extent;
(d) Duration refers to the incidents' length of time;
(e) Intent refers to the purpose behind the act(s) in question; and
(f) Context refers to the circumstances surrounding the incident.

Fidler [12] states that applying doctrinal analysis alone is insufficient to understand how international law applies to events. International lawyers must also consider how states respond to incidents because state practice helps reveal how states view such incidents politically and legally. States shape the meaning and interpretation of international legal rules through their behaviour, which is important in areas in which international agreements don't define concepts such as the use of force and armed attack [12].

5.2 Interpretation of International Law in Terms of the Tallinn Manual and Other Authors on When Conduct Constitutes Cyber Warfare

5.2.1 Tallinn Manual

Melzer [10] a participating expert to the Tallinn Manual gives a concise and clear summary of the application of international law to cyber warfare which makes for good reading.

Chapter II of the Tallinn Manual deals with use of force. The International Group of Experts discussed chapter II with reference to the International Court of Justice which stated that Article 2(4) of the UN Charter regarding the use of force (Rules 10–12 of the Tallinn Manual) and Article 51 of the UN Charter regarding the use of self-defense (Rules 13–17 of the Tallinn Manual) apply to 'any use of force regardless of the weapons employed.' The International Group of Experts unanimously agreed that cyber operations falls within the ambit of this statement and is an accurate reflection of the customary international law.

To determine whether cyber operations constitute use of force and armed attack, the Tallinn Manual refers to various rules. Since this discussion focuses on determining when conduct would constitute an act of war with specific reference to the attacks launched in 2007 on Estonia and 2010 on Iran, only those rules relevant to the discussion will be referred to.

A. *Ius ad bellum* (right to use force)

Regarding the use of force in terms of article 2(4) of the UN Charter:

Rule 11 provides that cyber actions will constitute use of force when its scale and effect are comparable to non-cyber operations rising to the level of a use of force. When it comes to use of force, the Tallinn Manual (Rule 13) refers to the following scenarios and whether it would amount to use of force:

- Non-destructive cyber psychological operations intended solely to undermine confidence in a government or economy will not qualify as a use of force.
- Funding a hacktivist group conducting cyber operations as part of an insurgency will not be use of force, but providing an organized group with malware and the training necessary to use it to carry out a cyber attack against another state will constitute use of force.
- Providing sanctuary (safe haven) to those mounting cyber operations of the requisite severity, will not be use of force but if the provision of sanctuary is coupled with other acts such as the substantial support or providing cyber defenses for the non-state group, it could in certain circumstances amount to use of force.

Rule 9 provides that a victim state may resort to proportionate countermeasures against the responsible state, for example if state B launches a cyber operation against state A's electricity generating facility at a dam in order to coerce state A to increase the flow of water into a river running through state B, state A may lawfully respond with proportionate countermeasures such as cyber operations against state B's irrigation system.

The International Group of Experts found that although the cyber operations against Estonia were persistent, the attack did not rise to the level of an armed conflict (Rule 20). The attack could also not be attributed to a specific nation-state as there was no confirmed evidence of attribution. As the attack brought down government websites, a major bank's online services and telephone networks it constituted a serious breach of the nation-state's security and its' critical information infrastructure. But within the ambit of the international law which recourse or remedy did Estonia have against the attack? The comment that the suspension by Estonia of some services to internet protocol (IP) addresses from Russia, is not considered as a countermeasure in terms of the Tallinn Manual, is interesting.

Although the International Group of Experts were unanimous that Stuxnet was illegal as an act of force in terms of article 2(4) of the UN Charter, they were divided on whether its effects were severe enough to constitute an 'armed attack.'

Regarding an armed attack in terms of article 51 of the UN Charter:

Had the use of the Stuxnet malware been an armed attack it would give rise to the right of unilateral self-defense on the part of Iran in accordance with article 51.

Rule 13 states that the scale and effects required for an act to be characterized as an armed attack necessarily exceeded those qualifying as use of force. Only in the event that the use of force reached the threshold of an armed attack is a state entitled to respond by using force in self-defense.

The International Group of Experts agreed that any use of force that injures or kills persons or damage or destroys property would satisfy the scale and effect requirement. They also agreed that acts of cyber intelligence gathering and cyber theft as well as cyber operations that involve brief or periodic interruption of non-essential cyber services do not qualify as an armed attack.

However, the International Group of Experts could not agree on whether or not actions that do not result in injury, death, damage, or destruction but would otherwise have extensive negative affect would constitute an armed attack. They were for example divided in respect of a cyber incident directed at the New York Stock Exchange that resulted in the market to crash: some felt that the mere financial loss did not constitute damage for purposes of an armed conflict whereas others were of the opinion that the catastrophic affect of such a crash, could constitute an armed attack. However, a cyber operation directed against major components (systems) of a state's critical infrastructure that caused severe, although not destructive effects, would qualify as an armed attack.

In respect of cyber espionage by state A against state B that unexpectedly results in significant damage to state B's critical infrastructure, the majority of the International Group of Experts agreed that intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter. Any response would however have to comply with the necessity and proportionality criteria (Rule 14) as well as

imminence and immediacy (Rule 15). The majority of the International Group of Experts agreed that a devastating cyber operation undertaken by terrorists (non-state actors) from within state A against the critical infrastructure located in state B qualified as an armed attack by the terrorists.

The majority of the International Group of Experts agreed that although article 51 does not provide for defensive action in anticipation of an armed attack, a state does not have to wait 'idly as the enemy prepares to attack', but it may defend itself if the armed conflict is imminent (anticipatory self-defense).

The International Group of Experts agreed that although there has not yet been a reported armed conflict that can be publicly characterised as having solely been precipitated in cyberspace, cyber operations alone have the potential to cross the threshold of international armed conflict.

B. *Ius in bello* (the law governing armed conflict)

A condition precedent to the application of the law of armed conflict is the existence of the armed conflict (Rule 20). The only example where the law of armed conflict was applicable to cyber operations was during the international armed conflict between Georgia and Russia in 2008 as the cyber operations were undertaken in the furtherance of that conflict. For instance if a hacker attack occurs after two countries become engaged in open conflict then the hackers behind the cyber attack have effectively joined hostilities as combatants and can be targeted with 'legal force' [8]. Although *ius in bello* is important, it is less relevant to the topic under discussion.

5.2.2 The Interpretation of International Law by Other Authors

In support of the interpretation given by the Tallinn Manual:

Joyner [14] agrees with the interpretation the Tallinn Manual gives to whether the use of the malware, Stuxnet constituted illegal intervention, illegal use of force and armed attack. He states that there has been a debate amongst international legal scholars over whether, and to what extent, the criteria for use of force under article 2(4) and the criteria for armed attack under article 51 differ. Joyner feels that there is a difference in intensity evidenced in the applicable legal sources. He is of the opinion that as the use of force was illegal in terms of article 2(4) it would allow Iran the right to engage in lawful countermeasures as defined in the law on state responsibility. Rule 9 of the Tallinn Manual suggests proportionate countermeasures are permitted against online attacks carried out by a state. Such measures cannot involve the use of force, however, unless the original cyber-attack resulted in death or significant damage to property. There must also be clear evidence that the target of the countermeasure is the state responsible for the illegal use of force. Evidence and attribution are some of the difficulties facing the legal regulation of cyber attacks. It should also be kept in mind that Iran did not know that its infrastructure was under attack or by whom until long after Stuxnet had done its damage [8].

Fidler [12] takes an interesting view of Stuxnet. As Stuxnet constituted a deliberate, hostile, highly sophisticated, state-created and critical infrastructure threatening offensive use of malware, he is of the opinion that by applying the criteria referred to at paragraph 5.1 to Stuxnet, a plausible argument can be made that its deployment constituted an illegal use of force, armed attack and an act of aggression. But he goes

on to say that although doctrinal analysis is important, state practice must also be taken into account. Fidler remarks that nation-states have curiously been quiet about Stuxnet. He indicates that nation-states such as the victim state (Iran), emerging great powers not suspected of involvement (for example China, Russia and India) and developing countries have refrained from applying international law on the use of force, armed attack and aggression. Fidler therefore comes to the conclusion that the state practice of silence suggests that from a legal and technical perspective states may not have perceived that this situation triggered the international rules on the use of force, armed attack and aggression.

He comes to the following conclusion - and one that may necessitate some debate - namely that after Stuxnet there may have been a development of cyber-specific rules that increase the political and legal space in which states can use cyber technologies against one another. In the light of state practice in the wake of Stuxnet, he suggests that especially big cyber-powers such as China, Russian and the US are seeking to establish higher use-of-force and armed-attack thresholds for cyber-based actions to permit more room to explore and exploit cyber technologies as instruments of foreign policy and national security. For example, states engage in cyber espionage on a scale, intensity and intrusiveness that signals a tolerance for covert cyber operations. Cyber espionage imposes adverse political, economic and military pressure on governments which in a physical world would have been considered illegal threats or uses of force. Therefore he argues that in the light of state practice, Stuxnet did not cross the threshold into use of force.

After the DDoS attacks on Estonia, the Estonian government argued that it was the victim of an armed attack but NATO and Russia opposed this characterization. [12] It should be noted that although Iran may not have publicly denounced the states responsible for the attacks as Estonia did, it did not accept the attacks without reprisals. It was reported in August 2012 that a virus infected the information network of the Saudi Arabian oil major, Aramco, and erased data on three-quarters of its corporate computers. All the infected screens were left displaying an image of a burning American flag. Chaulia [15] states that it was a symbolic counter-attack by Iran against the 'economic lifeline of a U.S ally and a deadly rival in the Middle East.' In the same article [15] it is reported that in September 2012 Iran launched a series of sequential attacks against the US financial industry including JP Morgan and Wells Fargo which resulted in the slowing down of overwhelmed servers and denying customers access to the bank services.

It is clear from Clarke and Knake's comments in respect of the launch of the Stuxnet worm that they are of the opinion that the conduct of the US was not in its best interest. The comments are interesting taking into account that Clarke was a former cyber-security advisor to President Obama. They state that with Stuxnet the US had crossed a Rubicon in cyber space. It launched a cyber attack that not only caused another nation's sensitive equipment to be destroyed, but it also legitimized such behaviour in cyberspace. It is however debatable whether the US and Israel succeeded in their object: the process only delayed the Iranian nuclear program by months. The biggest problem is that Stuxnet fell into the hands of hackers throughout the world who now have a sophisticated tool to attack the kind of networks that turn electrical power grids, pipeline networks, railways, and manufacturing processes in refineries and chemical plants.

6 The Way Forward Regarding the Governance of Conduct that Constitutes Cyber War

Melzer [10] concludes that although cyber warfare is subjected to established rules and principles within the ambit of the international law, transporting the rules and principles of international law that were developed in a physical world to cyber space pose some difficulties. He states that some of these questions require unanimous policy decisions by the international legislator, the international community of states.

I am of the opinion that this 'international legislator' will have to convene under the auspices of the United Nations. My opinion [16] is based on the following:

- The Council of Europe Convention on Cybercrime of 2001 (referred to as the Cybercrime Convention) which came into operation in 2004 have not reached a global level of acceptance by nation-states. In 2013 approximately 34 nation-states have become members of the Cybercrime Convention. South Africa was interestingly enough one of four states that participated in the drafting of the Cybercrime Convention. Since its implementation, South Africa became a member state in 2010 of the economic organization, BRICS which consists of Brazil, Russia, India and China. It is doubtful whether South Africa will ratify the Cybercrime Convention.
- In 2011 Russia, China, Tajikistan and Uzebikistan sent a letter to the UN Secretary-General Ban Ki-moon calling for a UN resolution on a code of conduct relating to the use of information technology by countries. [17] The proposed UN resolution called on countries to co-operate in order to combat criminal and terrorist activities involving cyberspace. It also called on countries to give an undertaking that it would not use technology to carry out hostile acts of aggression. The code provides that a nation-state should be in the position to protect their information 'space' and critical information infrastructure from threats, disturbance, attack and sabotage. Many states have developed cyber warfare capabilities [15].
- The purpose of the ITU World Conference on International Telecommunications (WCIT – 12) was to agree on updates to the International Telecommunications Regulations (ITR) which had last been discussed in 1988. Unfortunately the WCIT – 12 highlighted the tension between so-called western and non-western states in respect of internet regulation. On the one hand there is the so-called western nation-states under the leadership of the US who opposes international regulation. The US favours bi- and multi-national agreements between nation-states to address across border concerns, such as cybercrime investigations. Opposing this group of nation-states, the so-called non-western nation-states under leadership of Russia and China, propose a central international body to regulate cybercrime and cyber warfare [18].

Although the WCIT-12 was not the ideal forum to air the differences in respect of the legal regulation of the internet, it is inevitable that in the absence of any forum, the conflict – long expected – would openly come to the fore. One can only speculate on the root causes for the tension. Not only did internet connectivity of nation-states result in many nation-states of different cultural, economic and political views joining the international cyber environment, but it may be that some nation-states are of the opinion that as the internet is not owned by a specific nation-state that all nation-states

should participate as equal partners in the governance of cyberspace and this may have resulted in a power-struggle between nation-states for dominance of the internet.

7 Conclusion

The Tallinn Manual is a commendable document. It provides comprehensive rules pertaining to when conduct constitutes cyber warfare. It also shows that determining when and which conduct constitutes cyber warfare is complex and in some instances the position is far from certain. Similarly it is also not certain when a victim state may use countermeasures or act in private-defense against the state responsible for the attack.

Chaulia [15] states: 'Eventually, in the absence of any multilateral agreement at the level of the United Nations to moderate and set limits on cyber war, there could (be) a balance of power and a "balance of terror" that will set in to regulate the murky business of hacking and destroying the internet assets of adversaries.' This is apparent in the reprisals in respect of attacks that may not constitute cyber war in terms of the international law.

This discussion concludes with an extract of a speech by President Obama: 'But cyberspace has also been abused … Because cyber weapons are so easily activated and the identity of an attacker can sometimes be kept secret, because cyber weapons can strike thousands of targets and inflict extensive disruptions and damage in seconds, they are potentially a new source of instability in a crises, and could become a new threat to peace … And our goal as signers of the United Nations Charter is, as pledged in San Francisco well over half a century ago, to save succeeding generations from the scourge of war. I ask you to join me in taking a step back from the edge of what could be a new battle space and take steps not to fight in cyberspace but to fight against cyber war' [5].

These words are on the one hand quite ironic taking into account the US and Israel's co-operative launch of Stuxnet against Iran, but on the other hand the US now realizes its vulnerability with reference to Clarke and Knake who states: '… the US has launched also what is likely to be a cyber boomerang, a weapon that will someday be used to attack some of America's own defenceless networks' [5].

Unfortunately I am of the opinion that not all the internet-connected nations has heard the plea by the US or if they have, it is debatable whether there exists sufficient trust, confidence and transparency between nation-states to believe, in the absence of a multilateral treaty on cyber warfare, that a nation-state will uphold its' pledge not to use cyber warfare.

References

1. Schmitt, M.N.: Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press, Cambridge (2013)
2. Rauscher, K.F., Korotkov, A.: Russia-U.S. Bilateral on Critical Infrastructure Protection: Working towards Rules for Governing Cyber Conflict Rendering the Geneva and Hague Conventions in Cyberspace, p. 8, 11, 14, 18. EastWest Institute, New York (2011)

3. Zetter, K.: Legal experts: Stuxnet attack on Iran was illegal 'act of force' (2013). http://www.wired.com/threatlevel/2013/03/stuxnet-act-for
4. National Cybersecurity Policy Framework for South Africa (2013). http://www.cyanre.co.za/national-cybersecurity-policy.pdf
5. Clarke, R.A., Knake, R.K.: Cyber War, p. 6, 11–14, 278–279, 290–296. HarperCollins Publishers, New York (2012)
6. Kirchner, S.: Distributed Denial-of-Service Attacks Under Public International Law: State Responsibility in Cyberwar. In: The Icfai University Journal of Cyber law, p. 13. Icfai University Press, Hyderabad (2009)
7. Bowcott, V.: Rules of cyberwar: don't target nuclear plants or hospitals says NATO manual (2013). http://www.guardian.co.uk/world/2013/mar/18/rules-cyberw
8. Leyden, J.: Cyberwarfare playbook says Stuxnet may have been 'armed' attack (2013). http://www.theregister.co.uk/2013/03/27/stuxnet_cyverwar_r
9. Into the Intro: The Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). http://www.cambridgeblog.org/2013/04/into-the-intro-the-tal
10. Melzer, N.: Cyberwarfare and International Law (2011). http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf
11. Vihul, L.: The Tallinn Manual on the International Law applicable to cyber Warfare. http://www.ejiltalk.org/the-tallinn-manual-on-the-internation
12. Fidler, D.P.: Was Stuxnet an act of war? decoding a cyberattack. In: IEEE Computer and Reliability Societies, pp. 56–59 (July/August 2001)
13. Dugard, J.: International Law: A South African Perspective. Juta, Cape Town (2011). Chapter 24 (pp. 495–513) and chapter 25 (pp. 519–525)
14. Dan Joyner, D.: Stuxnet an "Act of Force" Against Iran". http://armscontrollaw.com/2013/03/25stuxnet-an-act-of-force-agains
15. Chaulie, S.: Cyber Warfare is the new threat to the global order (2013). http://www.nationmultimedia.com/opinion/Cyber-warfare-is
16. Watney, M.M.: The way forward in addressing cybercrime regulation on a global level. J. Internet Technol. Secur. Trans. **1**(1/2) (2012)
17. United Nations General Assembly, '66th session developments in the field of information and telecommunications in the context of international security'. http://www.chinadaily.com.cn/cndy/201109/14/content_13680896.htm. Accessed Feb 2012
18. Watney, M.M.: A South African legal perspective on State Governance of Cybersecurity within an African and global context. In: Lex Informatica, South Africa (2013)