You can't cyber in here, this is the War Room!

A rejection of the effects doctrine on cyberwar and the use of force in international law

Tobias Kliem

School of Law, Criminal Justice and Computing, Canterbury Christ Church University, Canterbury, UK

CONTACT: tobias.kliem@canterbury.ac.uk

ABSTRACT

There is a growing consensus in the literature on the applicability of the *jus ad bellum* to cyber-attacks that the effects caused by an attack should determine whether the attack constitutes a use of force (Article 2(4) of the UN Charter) or an armed attack giving rise to self-defence (Article 51 of the UN Charter). This article argues that this approach is inconsistent and dangerous. The push to include cyber-attacks in the existing framework on the use of force disregards the consensus on other non-conventional uses of force like economic sanctions and damage caused by espionage, and it is premised on dangerous hyperbole from in sensational media stories. Such an approach ignores serious practical problems regarding the attribution of cyber-attacks and would open the door wide for abuse. There is no reason to weaken the effectiveness of a deliberately narrow system on the use of force based on dystopian scenarios.

KEYWORDS

use of force; armed attack; self-defence; cyberwar; hacking

1. Introduction

Cyberwar[1] and computer network attacks have had a lot of attention and interest in the recent years. The concerted Distributed Denial of Service (DDoS) attacks against a wide range of Estonian websites, the well-documented Stuxnet worm, and the partially related revelations concerning the United States' mass espionage activities by Edward Snowden have made it clear to governments, academics, journalists and the wider public that 'cyber' is an area that matters when it comes to the wars of the future.

[1] While the tendency of journalists and politicians to use the prefix 'cyber' for almost everything is rightly looked down upon in Computer Science circles, it has become almost a convention to speak of 'cyber-attacks' and 'cyberwar'. Accordingly, these words will be used in the following article.

Politicians are not shy of drastic comparisons in this regard. Leading American officials like Richard Clarke, the then National Coordinator for Security Infrastructure Protection and Counter-terrorism with the National Security Council,[2] and Leo Panetta, the former Director of the CIA and at that time the US Secretary of Defence,[3] have referred to the threat of a 'cyber [or electronic] Pearl Harbour' that is looming over the United States. Many states have set up cyber divisions within their armed forces, establishing both offensive and defensive capabilities.[4]

Obviously, this matter was not a central concern to the creators of the UN Charter or of the Geneva Conventions (even though computers and computer aided espionage played a big role in the Second World War), so a much debated topic at the moment is how cyber-attacks fit into the international legal framework of warfare. A plethora of articles and a number of books have already been written on the applicability of *jus ad bellum* (the rules on the legality of a war itself),[5] of *jus in*

---

[2] Eric Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 *Stanford Journal of International Law* 207, 211.

[3] 'Leon Panetta Warns of "Cyber Pearl Harbour"', *BBC News* (12 October 2012) www.bbc.co.uk/news/technology-19923046 (accessed 30 June 2015).

[4] Aerie J Schaap, 'Cyber Warfare Operations: Development and Use under International Law' (2009) 64 *The Air Force Law Review* 121, 127 et seq; Richard Stiennon, 'A Short History of Cyber Warfare' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015) 7, 22–7.

[5] See, e.g. Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 *New York University Journal of International Law and Politics* 57; Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification' (2009) 1 *Goettingen Journal of International Law* 375; Lianne J M Boer, 'Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace' (2013) 5 *Amsterdam Law Forum* 4; Davis Brown, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 *Harvard International Law Journal* 179; Gary Brown and Keira Poellet, 'The Customary International Law of Cyberspace' (2012) *Strategic Studies Quarterly* 126; Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict and Security Law* 211; Yoram Dinstein, 'Computer Network Attacks and Self-Defense' in Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College, 2002) 99; Jenny Dröge, 'Cyber Warfare: Challenges for the Applicability of the Traditional Laws of War Regime' (2010) 48 *Archiv des Völkerrechts* 486; David P Fidler, 'Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law' (2012) 16(22) *ASIL Insights*, www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and (accessed 26 May 2017); Dieter Fleck 'Searching for International Rules Applicable to Cyberwarfare – A Critical First Assessment of the New Tallinn Manual' (2013) 18 *Journal of Conflict and Security Law* 331; Matthew Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right to Self-Defense' (2009) 32 *Boston College International and Comparative Law Review* 439; Jensen (n 2); Herbert S Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 *Journal of National Security Law and Policy* 63; Reese Nguyen, 'Navigating *Jus ad Bellum* in the Age of Cyber Warfare' (2013) 101 *California Law Review* 1079; Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 *Journal of Conflict and Security Law* 187; Titiriga Remus, 'Cyber Attacks and International Law of Armed Conflicts; a "Jus ad Bellum" Perspective' (2013) 8 *Journal of International Commercial Law and Technology* 179; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 43–116; Schaap (n 4); Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885; Michael N Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (2011) 56 *Villanova Law Review* 569; Michael N Schmitt, 'International Law in Cyberspace: The Koh Speech and the Tallinn Manual Justaposed' (2012) 54 *Harvard International Law Journal Online* 13; Scott J Shackleford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' (2009) 27 *Berkeley Journal of International Law* 192; P W Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014); Nicholas Tsagourias 'Cyber attacks, Self-Defence, and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229; Anna Wortham, 'Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?' (2011) 64 *Federal Communications Law Journal* 643.

bello (the rules governing the conduct in a war),[6] and some articles have been dedicated to the applicability of international criminal law to cyber-attacks[7]. This article is focusing on *jus ad bellum*.

While there is a wide range of different articles and books on this topic, and while these differ in their methodologies and argumentations, there appears to be one consensus in an overwhelming majority of them: what matters for the qualification of an attack under international law is not so much related to which methods were used to commit it, but what effect was caused by it. For the purpose of this article, this view is referred to as the 'effects doctrine'.

On first glance, the doctrine seems entirely logical. If a person gets hurt by someone else, it is ultimately not important to that person whether this was done by being pushed down a flight of stairs, by being intentionally run over with a car or by being beaten with a cricket bat. What matters would indeed be the effect – the amount of pain and the injuries caused.

However, this article argues that the effects doctrine should not be applied to cyber-attacks. This application would endanger the traditional approach to the use of force in international law, would be inconsistent with the understanding of the use of force in other areas and would ultimately be quite dangerous. The cyberwar scenario that is reflected in many articles (both in mass media and in academic publications) is overstated, and a response not involving the traditional *jus ad bellum* would be more appropriate and more in line with the goals of the United Nations.

To make this argument, the article will first, in section 2, summarise the effects doctrine. Section 3 will then go on to show that the doctrine is inconsistent, because an effects based approach has been rejected by the leading opinion on the use of force when it comes to economic sanctions. The way states treat espionage is similarly problematic, as states deliberately chose not to include

---

[6] See, e.g. Jack M Beard, 'Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law' (2014) 47 *Vanderbilt Journal of Transnational Law* 67; Yoram Dinstein, 'The Principle of Distinction and Cyber War in International Armed Conflicts' (2012) 17 *Journal or Conflict and Security Law* 261; Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533; Herbert Lin, 'Cyber Conflict and International Humanitarian Law' (2012) 94 *International Review of the Red Cross* 515; Jeremy Richmond, 'Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?' (2012) 35 *Fordham Journal of International Law* 842; Lesley Swanson, 'The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict' (2010) 32 *Loyola LA International and Comparative Law Review* 303; Wissenschaftlicher Dienst des Deutschen Bundestages, 'Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare)' (2015) WD 2 – 3000 – 038/15; Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis and Theodoros Apostolopoulos, 'Cyberoperations and International Humanitarian Law: A Review of Obstacles in Applying International Law Rules in Cyber Warfare' (2016) 24 *Information & Computer Security* 38;; Roscini (n 5) 117–245; Michael N Schmitt, 'Cyber Operations and the *Jus in Bello*: Key Issues' (2011) 87 *International Law Studies* 89; Michael N Schmitt and Sean Watts, 'The Decline of International Humanitarian Law *Opinio Juris* and the Law of Cyber Warfare' (2015) 50 T*exas International Law Journal* 189; Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff, 2013); Katharina Zielowski, 'Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen' (2008) 21 *Humanitäres Völkerrecht – Informationsschriften* 202.

[7] See, e.g. Chance Cammack 'The Stuxnet Worm and Potential Prosecution by the International Criminal Court under the Newly Defined Crime of Aggression' (2011) 20 *Tulane Journal of International and Comparative Law* 303.

espionage and related incidents below a certain threshold in the use of force framework. The doctrine is further inconsistent in its application, as the effect does not only depend on the attack used, but also on the victim state. The other major problems with the effects doctrine are practical: it is argued in section 4 that it is only in very rare instances possible to identify the perpetrator and to identify the intention of that perpetrator with a certainty that should be required for decisions of this magnitude. Finally, it is necessary to consider whether the danger that many writers portray is really existent. The article will therefore examine, in section 5, the examples used within the cyber war debate, and show that the different scenarios that are discussed in almost all academic (and media) elaborations of the topic are unrealistic or hyperbolic. Basing a potential extension of the framework governing the use of force on hyperboles and unrealistic fear is not the most helpful contribution to making the world a safer place. Instead, the conclusion will argue, we should rely first and foremost on an international effort to improve computer security, and on responses below the use of force threshold. The cyberwar debate needs to leave the realms of the military.

2. The effects doctrine

The basic rules of the international legal framework on the use of force seem quite straightforward and are probably well known to any reader of this journal. Therefore, the summary in this section will be very brief.

Under Article 2(4) of the Charter of the United Nations (UNC), the 'use of force' and the threat of that use are prohibited. It is widely accepted that this article also reflects customary international law, and it is seen as a provision of *jus cogens*, a norm of international law that cannot be overridden by treaty or custom.[8] Besides the now obsolete case of the use of force against former enemy states in Article 107 UNC, the Charter allows only two exceptions from this prohibition: authorisation by the Security Council under Chapter VII of the Charter and self-defence under Article 51 UNC. The latter is, according to the Charter, only permissible 'if an armed attack occurs'.

The UN Charter was written in 1945, in the immediate aftermath of the two world wars. What the founders of the United Nations had in mind when they wrote the words 'use of force' and 'armed attack' were no doubt images like Hitler's tanks driving over the Polish border or Japanese planes bombing Pearl Harbour. Therefore, the question of whether the typing of a string of commands into the terminal window of a computer can constitute a use of force or an armed attack is a complex one.

---

[8] *Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v United States of America*) (merits) [1986] ICJ Rep 14, para 190. See also Oliver Dörr 'Use of Force, Prohibition of' (2015) *Max Planck Encyclopedia of Public International Law*, online version, http://opil.ouplaw.com/home/EPIL, para 1 (accessed 19 April 2017); Christine Gray, *International Law and the Use of Force* (Oxford University Press, 3rd edn 2008) 30.

After the topic of cyberwar became more prominent in the media, a number of writers started to assess in how far these actions are covered by the current international legal framework. Most importantly, an 'International Group of Experts' convened in Tallinn at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence to write the 'Manual on the International Law Applicable to Cyber Warfare', or 'Tallinn Manual'. The Manual was originally published in 2013,[9] and then, in 2017, was notably revised, expanded and updated (with the 2017 version being coined the 'Tallinn Manual 2.0').[10]

Although the Tallinn Manual itself points out that it 'is not an official document, but rather the product of two separate endeavours [i.e. the production of the Tallinn Manual and the Tallinn Manual 2.0] undertaken by groups of independent experts acting solely in their personal capacity',[11] and that it 'does not represent the views of NATO',[12] the Manual has had considerable influence. Michael Schmitt, the Manual's General Editor, claims it reflects 'teachings of the most highly qualified publicists',[13] a direct reference to one of the sources of international law as listed in Article 38(1) of the Statute of the International Court of Justice. Much of the Manual is based strongly on Schmitt's previous writings,[14] in particular his article 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' written in 1999.[15]

The most important part of the Manual concerning the *jus ad bellum* is contained in Tallinn Manual 2.0 Rules 69 (Rule 11 in the 2013 version) and 71 (Rule 13 in the 2013 version), assessing how cyber operations can be a use of force (Rule 69) and an armed attack (Rule 71). Rule 69 borrows a phrase used by the International Court of Justice (ICJ) in its *Nicaragua* judgment (albeit in a different context): the 'scale and effects' of the attack should be the qualifying factor.[16] The Manual distinguishes two kinds of effects: first, it unambiguously states that acts that 'injure or kill persons or damage or destroy objects *are* uses of force'.[17] For operations below that threshold, the Manual suggests a set of criteria that 'states are likely to consider'[18] when assessing if it there has been a use of force: severity (the act should constitute more than a 'mere inconvenience or irritation'); immediacy (the faster the effect of a cyber operation manifests itself, the more likely it is that it is a use of force); directness (the effects should be caused by the operation itself, not by other factors);

---

[9] Michael N Schmitt (gen ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).
[10] Michael N Schmitt (gen ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2nd edn 2017).
[11] *Ibid*, 2.
[12] *Ibid*.
[13] Schmitt, 'International Law in Cyberspace' (n 5) 15.
[14] Boer (n 5) 6.
[15] Schmitt, 'Computer Network Attack and the Use of Force in International Law' (n 5) 885.
[16] *Tallinn Manual 2.0* (n 10) 331.
[17] *Ibid*, 333 (emphasis added).
[18] *Ibid.*

invasiveness (the more secure the system infiltrated, the higher the likeliness of the act being a use of force); measurability (the consequences should be apparent); military character; state involvement; and the illegality of the act.[19]

While not every one of these criteria is reflected in every journal article on the topic, the general idea that the effects of an operation determine whether it constitutes a use of force has found the widespread appreciation of many academics,[20] and is considered the 'majority view'.[21] Singer and Friedman write '[i]f your power plant explodes in a fiery blast that kills thousands, whether the cause was an actual bomb or logic bomb is not a major distinguishing factor'.[22]

The Tallinn Manual applies the same principle to Article 51 UNC as well. According to Rule 71 of the Manual, decisive for the question whether a cyber-attack is an 'armed attack', allowing states to act in self-defence, are again 'scale and effects'.[23] The ICJ, in its *Nicaragua* decision, distinguished an 'armed attack' from the 'use of force' by stating that only the 'most grave forms' of the use of force should constitute an armed attack.[24] The requirement of gravity has been taken up again by the Court in the *Oil Platforms* case.[25] It also is supported by many scholars,[26] but is strongly disputed by others, most notably by American officials.[27]

Therefore, the Tallinn Manual takes note of some disagreements within the group of experts on the scale and effects required, but makes clear that the experts decided unanimously that 'some cyber operations may be sufficiently grave to warrant classifying them as an "armed attack"'.[28] As with Rule 69, acts that result in the death or injury of persons or in the destruction of property do, in the eyes of the group of experts, qualify as armed attacks.[29] Many scholars have agreed in principle with this position.[30] Hoisington, for example, sees it as necessary for deterrence that states are allowed to use self-defence against cyber-attacks 'without being restrained by outdated interpretations of international law governing the use of force'.[31] Jensen goes even further and write that 'in the age of

---

[19] *Ibid*, 333–6.
[20] See, e.g. Brown (n 5) 187; Wortham (n 5) 651; Barkham (n 5) 79; Roscini (n 5) 62; Remus (n 5) 188 et seq; Shackleford (n 5) 231.
[21] Johann-Christoph Woltag, 'Cyber Warfare' (2010) *Max Planck Encyclopedia of Public International Law*, online version, http://opil.ouplaw.com/home/EPIL, para 8 (accessed 19 April 2017).
[22] Singer and Friedman (n 5) 125.
[23] *Tallinn Manual 2.0* (n 10) 339.
[24] *Nicaragua* (merits) (n 8) para 191.
[25] *Case Concerning Oil Platforms* (*Islamic Republic of Iran v United States of America*) (merits) [2003] ICJ Rep 161, para 51.
[26] See, e.g. Albrecht Randelzhofer and Georg Nolte, 'Article 51' in Bruno Simma (ed), *The Charter of the United Nations* (Oxford University Press, 3rd edn 2012) para 20.
[27] See, e.g. the article by the then State Department Legal Adviser: William H Taft, 'Self-Defense and the Oil Platforms Decision' (2004) 29 *Yale Journal of International Law* 295, 300 et seq.
[28] *Tallinn Manual 2.0* (n 10) 340.
[29] *Ibid*, 341.
[30] Tsagourias (n 5) 231; Woltag (n 21) para 9; Brown (n 5) 188; Barkham (n 5) 80; Remus (n 5) 188 et seq; Schaap (n 4) 147 et seq; Shackleford (n 5) 237.
[31] Hoisington (n 5) 454. See also Jensen (n 2) 228.

instantaneous computer lethality', states should also have the right to use anticipatory self-defence against imminent cyber-attacks.[32] This should, in his eyes, even apply to attacks below the 'armed attack' threshold (relying on the theory that Article 51 UNC is only a codified version of a wider customary right to self-defence).[33] Roscini is a bit more careful and qualifies that 'only large scale cyber attacks on critical infrastructures that result in significant physical damage or human losses comparable to those of an armed attack with conventional weapons' allow self-defence,[34] but ultimately, his view also stands firmly within the effects doctrine.

It needs to be pointed out that while a response in self-defence must be proportionate to the attack, it is not limited to the same means/methods as that attack. A proportionate response to a cyber-attack could, according to one scholar, consist, for example, of 'precision bombing against known cyber warfare operation centres'.[35]

This discussion is by no means limited to the academic world. A number of states, including the United States,[36] the United Kingdom,[37] and Germany,[38] have made it clear that they are willing to respond to cyber-attacks on critical military infrastructure with military force.[39] The former President of the United States, Barack Obama, explicitly referred to the right of self-defence when talking about cyber threats and stated that the US 'reserve[s] the right to use all necessary means – diplomatic, informational, military, and economic' to defend the country.[40] Similarly, the Secretary-General of NATO has pointed out that in his view a cyber-attack can trigger collective self-defence under Article 5 of the North Atlantic Treaty.[41]

The proponents of the effects doctrine typically list two older sources as support for their position. Obviously, cyber warfare is not the first scenario that does not quite fit into the wording of Articles 2(4) and 51 UNC. Ian Brownlie famously considered attacks involving the use of non-

---

[32] Jensen (n) 221. See Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (n 5) 593.
[33] Jensen (n 2) 229.
[34] Marco Roscini, 'World Wide Warfare – *Jus ad bellum* and the Use of Cyber Force' (2010) 14 *Max Planck Yearbook of United Nations Law* 85, 130.
[35] Schaap (n 4) 149. See also Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (n 5) 594.
[36] US Department of Defense, 'The DoD Cyber Strategy' (2015) www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 11 (accessed 24 February 2017).
[37] HM Government, 'National Cyber Security Strategy 2016–2021' (2016) www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, 47, 49 et seq (accessed 5 March 2017).
[38] See Bundesregierung der Bundesrepublik Deutschland, 'Weissbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr' (2016) www.bmvg.de/resource/resource/UlRvcjZYSW1RcEVHaUd4cklzQU4yNWFvejhLbjVyYnR1OCt3ZlU1N09FVkZoYmR4Sjljb1E2UW9BdC9qQ3U1bmVEck9CbDgvcUFZaUhSL1dSSFA0alRxelpqQ3dyK1E3LzB4N0lXQ0lhcHM9/Weissbuch2016_barrierefrei.pdf, 36, 56, 65 (accessed 24 February 2017).
[39] Roscini (n 5) 74 et seq.
[40] 'International Strategy for Cyber Space: Prosperity, Security, and Openness in a Networked World', *White House* (May 2011) www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 14 (accessed 20 July 2015).
[41] Press Conference by Jens Stoltenberg (14 June 2016), www.nato.int/cps/en/natohq/opinions_132349.htm (accessed 8 February 2017).

conventional weapons like chemical or biological substances, and concluded that the 'destruction to life and property' should form the litmus test for asserting a use of force and an armed attack.[42] Likewise, the ICJ held in its advisory opinion on *Nuclear Weapons* that Articles 2(4) and 51 UNC 'do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed'.[43] The Court explicitly refers to new weapon systems when writing on the applicability of International Humanitarian Law:

> However, it cannot be concluded ... that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[44]

3. The inconsistency of the effects doctrine

Basing the evaluation of cyber-attacks merely on their effect is, however, inconsistent with regards to other potential attacks that could be committed by states, most notably the use of economic force and the grey area of espionage and sabotage. It is, further, problematic that the evaluation of the effects of a cyber-attack depends strongly on the victim state.

3.1. Economic sanctions

One of the longest debates on the non-conventional uses of force is the use of economic force, a topic that has been discussed since the San Francisco Conference. The leading opinion among politicians and scholars about the use of economic force has always been that the use of economic force is not included in Article 2(4), and even less so in Article 51,[45] although there is a notable difference between writers from developed countries (who tend to agree with the proposition that economic force is not 'force') and writers from developing countries (who tend to disagree with this position).[46]

The strongest argument to include the use of economic and political force in the scope of Article 2(4) is a textual one: it is remarkable that the authors of the Charter chose to use the rather general words 'use of force' without further qualification in Article 2(4), even though the more

---

[42] Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, 1963) 362.
[43] *Legality of the Threat or Use of Nuclear Weapons* (advisory opinion) [1996] ICJ Rep 226, para 40.
[44] *Ibid*, para 86.
[45] See, e.g. Dörr (n 8) para 11.
[46] Christine Gray, 'The Use of Force and the International Legal Order' in Malcolm Evans (ed), *International Law* (Oxford University Press, 2006) 589, 592.

specific phrase 'armed force' is used three times elsewhere in the Charter (in the preamble and in the Articles 41 and 46). The words 'armed attack' in Article 51 of the Charter also signify a distinction to the mere 'use of force'. Asserting that 'force' means 'armed force' would, according to Paust and Blaustein, equate to reading something in the text that is not there.[47]

However, this argument is usually rejected based upon the *travaux préparatoires* of the Charter: the San Francisco Conference rejected a Brazilian proposal to explicitly include economic coercion within the use of force ('*ou aux menaces ou à l'émploi de mesures d'ordre économique incompatibles*').[48] The Friendly Relations Declaration, one of the General Assembly Resolutions frequently used as an authoritative interpretation of Article 2(4), reminds states in its preamble that they have a duty to refrain from military, economic and political coercion in their international relations, but continues in its operative part to refer to force only in military terms.[49] It is assumed that the exclusion of economic uses of force also extends to the prohibition of the use of force in customary international law.[50]

Despite the convincing points made by the proponents of the textual interpretation, the explicit rejection of the Brazilian proposal is a clear indication for the intentions of the majority of the San Francisco Conference. According to Article 32 of the 1969 Vienna Convention on the Law of Treaties, preparatory work of the treaty can be taken into account when the normal interpretation 'leaves the meaning ambiguous or obscure'. As much as a wider perspective on 'force' might be desirable from a moral standpoint, such a perspective would ignore the intentions of the Charter's drafters. There is also nothing in the subsequent practice of the majority of states that would indicate a change in this position.

Ultimately, this debate does not have to be solved at great length in this article, as it is not the main subject of discussion here. Important for the purpose of this article, however, is the fact that many of the advocates of the effects doctrine, most notably the International Group of Experts that drafted the original version of the Tallinn Manual, uphold that the use of force in Article 2(4) does not include economic force. Rule 11 of the 2013 version of the Manual states that 'whatever "force" may be, it is not mere economic or political coercion'.[51] This wording was notably removed from the equivalent Rule 69 in the 2017 2.0 version[52] – injecting some ambiguity into the view of the Manual's

---

[47] Jordan J Paust and Albert P Blaustein, 'The Arab Oil Weapon – A Threat to International Peace' (1974) 68 *American Journal of International Law* 410, 415 et seq.
[48] UNCIO VI, 334, 609; Albrecht Randelzhofer and Oliver Dörr, 'Article 2(4)' in Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, and Andreas Paulus (eds), *The Charter of the United Nations A Commentary*, vol I (Oxford University Press, 3rd edn 2012) para 18.
[49] UNGA Res 2625 (XXV), UN Doc A/RES/2625 (XXV) (24 October 1970); Randelzhofer and Dörr (n 48) para 19.
[50] Dörr (n 8) para 12.
[51] *Tallinn Manual* (n 9) 4.
[52] *Tallinn Manual 2.0* (n 10) 331.

authors on this point – although it remains clear that the Manual still broadly ties its understanding of 'force' in the cyber context to the traditional position that economic and political coercion are excluded from the scope of Article 2(4), at least as a presumptive approach.[53] One of the best known writers on the use of force in international law, Yoram Dinstein, adopting the approach from the 2013 version of the Manual, also rejects the application of Article 2(4) to economic measures, but states that computer attacks can be uses of force if 'the end result [is] that violence occurs or is threatened'.[54]

The 2013 version of the Tallinn Manual (although not the 2017 2.0 version) similarly states that '[c]yber operations that involve, or are otherwise analogous to, [economic or political coercion] are definitely not prohibited uses of force'.[55] However, the original version of the Manual did not clarify the obvious contradiction: it held that cyber-attacks are uses of force if they 'injure or kill persons or damage or destroy objects',[56] but economic coercion can never be a use of force, even though its effects can injure or kill persons (for example, in the case of an export ban on food or medication), and have done so in the past.[57]

Economic warfare can have similar effects to those ascribed to cyber warfare, and it can have effects that are similar to armed attacks.[58] Moreover, contrary to most of the cyber-attack scenarios described in the literature, most economic sanctions are very indiscriminate in their application. Contrary to attacking military targets via cyber means (for example, causing a malfunction that leads to a military airplane crashing), which would clearly be a use of force or an armed attack following the Tallinn Manual, an economic sanction can affect very large parts of the population, often with disproportionate harm falling on the poorest parts of it.[59] Economic sanctions can also have similar effects on the freedom of information to the disruption of communication networks through a cyber-attack.[60] And economic sanctions can cause severe political distortion; one example is the 'major contribution' economic sanctions brought to the fall of Allende's government in Chile.[61]

It is certainly paradoxical to say that economic measures can *never* be uses of force, regardless of their effect, and that cyber-attacks can be uses of force because of their effect.[62] The effects of economic attacks are often secondary rather than immediate, but so are the effects of many of the

---

[53] *Ibid*.
[54] Yoram Dinstein, *War, Aggression and Self-Defence* (Cambridge University Press, 5th edn 2012) 88.
[55] *Tallinn Manual* (n 9) 46.
[56] *Ibid*, 48; *Tallinn Manual 2.0* (n 10) 333.
[57] See, e.g. Hartmut Brosche, 'The Arab Oil Embargo and United States Pressure Against Chile: Economic and Political Coercion and the Charter of the United Nations' (1974) 7(1) *Case Western Reserve Journal of International Law* 3, 4.
[58] Paust and Blaustein (n 47) 416.
[59] See, e.g. Seung-Whan Choi and Shali Luo, 'Economic Sanctions, Poverty and International Terrorism: An Empirical Analysis' (2013) 39 *International Interactions* 217, 220 et seq.
[60] See Dursun Peksen, 'Coercive Diplomacy and Press Freedom: An Empirical Assessment of the Impact of Economic Sanctions on Media Openness' (2010) 31(4) *International Political Science Review* 449.
[61] Brosche (n 57) 15.
[62] See also Boer (n 5) 10; Barkham (n 5) 92; Hoisington (n 5) 448 et seq.

cyber-attacks that have occurred or that are envisaged in the literature (a cyber-attack on an electrical grid, for example, is not destructive because of exploding transistors or burning relay stations, but because of the panic that it can cause). This likely explains why the 2017 2.0 version of the Tallinn Manual removed the categorical statements to the effect that cyber-attacks that solely involve economic and political effects can never amount to a use of force, albeit that the apparent *presumption* that they will do not remains a feature of the Manual.[63]

Dinstein's point that 'violence' is the difference[64] is not very convincing. It merely replaces one ambiguous and difficult to interpret word ('force') with another ('violence'). It is not difficult to argue that the act of cutting off the supply of life saving medication to a population has a better claim to the label 'violent' than the remote destruction of a weapon system.

Roscini tries to justify the different application of the effects doctrine by differentiating between the means and the target: sanctions use the economy 'as a *means* of pressure', cyber-attacks use it as the '*target*'.[65] A cyber-attack against a stock exchange is, according to him, more comparable with its bombing than with economic sanctions.[66] Again, this argument is not very convincing from the standpoint of an effect based approach on cyber-attacks. The devastating effects of a foreign power bombing the building of a stock exchange would not be the physical destruction of the building itself, but the economic distortion caused by the disruption of its operations. The economy would be used as a means of pressure in a very similar way to economic sanctions. This becomes even more obvious when looking at other writers who explicitly state that a cyber-attack on the financial system clearly constitutes an armed attack because of the following 'massive disruption to the economic life of a State'.[67]

Ultimately, if the effect of an attack were to be the decisive factor for both Article 2(4) UNC and Article 51 UNC, the approach to economic sanctions would have to be reshaped as well. The member states of the United Nations would need to come up with a clearer definition of these terms than the lowest common denominators that have been used for the Definition of Aggression and for the Friendly Relations Declaration.

3.2. Espionage and sabotage

Espionage and sabotage existed long before the proclaimed era of cyber warfare. The Cold War period, for example, is rich in anecdotes where covert action was used to cause physical damage. One of the earliest alleged computer attacks is the explosion of a Soviet pipeline in 1982 that, according

---

[63] See *Tallinn Manual 2.0* (n 10) 331.
[64] Dinstein (n 54) 88.
[65] Roscini (n) 62 (emphasis in original).
[66] *Ibid*.
[67] Tsagourias (n 5) 231.

to a member of the National Security Council at the time, was caused by intentionally faulty American software stolen by the Soviets.[68] During World War II, the United States' Strategic Services released a 'Simple Sabotage Field Manual', which makes very entertaining reading, and gives handy tips to any potential saboteur on what weapons to use ('salt, nails, candles, pebbles, thread, or any other materials he might normally be expected to possess as a householder or as a worker in his particular occupation') or what excuse to make after dropping a wrench into an electric circuit ('an air raid had kept you up the night before and you were half-dozing at work').[69]

Espionage is an area that is surprisingly unregulated in international law.[70] States have always regarded espionage as a necessity and have hence never shown any interest in legally restricting these practices.[71] Generally, it is accepted that spying is not considered a violation of international law,[72] but is an area that concerns domestic criminal law. There have been arguments that espionage in peacetime can constitute a violation of the rules of the territorial integrity of a state,[73] but these are in the minority. There is also no convincing argument to consider espionage, a wide spread practice amongst states,[74] as a violation of the prohibition of use of force or as an armed attack.[75] It is even possible to speak about an 'international norm of ignoring espionage activities'.[76]

The situation with sabotage is slightly different. Sabotage, particularly in a terrorist context, can be seen as a violation of Article 2(4) and as an armed attack under Article 51. It is, however, unclear whether a certain threshold has to be crossed in the sabotage act (or when it comes to any state action in general – e.g. poisoning an individual, shooting via drone or disrupting production) and if there is a *de minimis* exception to Article 2(4). According to Ruys, 'any deliberate projection of lethal force onto the territory of another state' is enough to trigger Article 2(4).[77] The existence of a *de minimis* exception has also been disputed in the context of terrorist attacks.[78]

---

[68] Alex Russell, 'CIA Plot Led to Huge Blast in Siberian Gas Pipeline', *The Telegraph* (28 February 2004) www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html (accessed 27 August 2016).
[69] US Office of Strategic Services, *Simple Sabotage Field Manual* (1944) www.gutenberg.org/files/26184/page-images/26184-images.pdf (accessed 27 August 2016).
[70] See Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection' (2011) 5 *Journal of National Security Law & Policy* 179, 204 et seq; Glenn Sulmasy and John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2006) 28 *Michigan Journal of International Law* 625.
[71] *Ibid*, 625; Christian Schaller, 'Spies' (2015) *Max Planck Encyclopedia of Public International Law*, online version, http://opil.ouplaw.com/home/EPIL, para 2 (accessed 19 April 2017).
[72] Lin (n 5) 72.
[73] See Manuel R Garcia-Mora, 'Treason, Sedition and Espionage as Political Offenses under the Law of Extradition' (1964) 26 *University of Pittsburgh Law Review* 65, 79 et seq.
[74] Robert D Williams, '(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action' (2011) 79(4) *The George Washington Law Review* 1162, 1163.
[75] Sulmasy and Yoo (n 70) 628.
[76] Todd A Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the UN Charter' (1998) 30 *Case Western Reserve Journal of International Law* 567, 581.
[77] Tom Ruys, 'The Meaning of "Force" and the Boundaries of the *Jus ad Bellum*: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?' (2014) 108(2) *American Journal of International Law* 159, 160.
[78] Christian J Tams, 'The Use of Force Against Terrorists' (2009) 20(2) *European Journal of International Law* 359, 375.

In a reply to Ruys' article, however, O'Connell rightfully argues that assuming such a wide scope of Article 2(4) (and, consequently, of Article 51) creates more opportunities for states to lawfully use force.[79] The legal understanding of a targeted killing operation, for example, would be quite different whether it consists of a drone strike with anti-tank missiles or in the covert stabbing done by a secret agent – in one case states would consider it a use of force and in the other a violation of human rights laws and the non-intervention principle.[80] When it comes to cyber-attacks, the Tallinn Manual applies a *de minimis* threshold as well: according to its authors, events 'generating mere inconvenience or irritation will never' be considered as a use of force.[81]

This creates a constant source of inconsistency. As will be discussed in section 5, many of the discussed cyber cases and scenarios operate along the blurry line between espionage and warfare, and it is often only the invisible and scary nature of a cyber-attack that makes writers focus on Article 2(4) rather than the individual criminal responsibility of the perpetrator.

3.3. The implications of differences between victim states

Another problem with the effects based approach to cyber-attacks is that the development of the victim is decisive for the effects caused by a cyber-attack.[82] This is obvious when looking at the descriptions of Estonia as 'the most wired country in Europe', which highlight that it is/will be disproportionately more affected by cyber-attacks than other states.[83] A computer attack on a less developed country might not cross the line of a use of force following the effects doctrine as outlined in section 2.[84] The same applies to a state like China, which has the capacity to cut itself off from the internet.[85]

We, therefore, are in the situation where a cyber-attack on the United States could be seen as a violation of Article 2(4), while the same attack on Mongolia would not. This is certainly not the case with traditional kinetic attacks: a bombardment of a city would qualify as an armed attack regardless of whether we are talking about a modern city with skyscrapers or about a city consisting of wooden huts, and tanks shooting on army barracks would be considered an armed attack regardless of whether the army barracks contain modern fighter planes or rusty muskets. A legal framework that

---

[79] Mary Ellen O'Connell, 'The True Meaning of Force' (2014) 108 *American Journal of International Law Unbound* 141, 142.
[80] *Ibid*, 144.
[81] *Tallinn Manual 2.0* (n 10) 334.
[82] Nguyen (n 5) 1124.
[83] Joshua Davis 'Hackers Take Down the Most Wired Country in Europe', *Wired* (2007) www.wired.com/2007/08/ff-estonia/ (accessed 4 August 2016).
[84] Nguyen (n 5) 1124.
[85] *Ibid.*

reaches different evaluations depending on the technological development of the victim state is, therefore, at least problematic.

4. Practical problems with the effects doctrine

4.1. Difficulty in detecting the origin of the attack

One of the biggest problems with expanding the framework on the use of force to include cyber-attacks is that it is very easy to disguise origins on the internet. Even unsophisticated spammers and teenage attention seekers are able to use a wide variety of tactics readily available on the internet. Camouflaging the origins of an attack is not difficult,[86] and is usually done by operating attacks from hijacked computers in other countries that are themselves accessed over multiple stages.[87] The attacks on Estonia,[88] for example, were launched from one million computers in over 100 countries.[89] This would be even more of a problem if the attack came from the well-equipped cyber department of an actual army, as many of the scenarios envisage. The usual way to identify perpetrators of malevolent internet activity does not work here: most cybercriminals are found by 'following the money', but in the case of a cyberwar there is no money trail to be followed.[90]

Even if it is possible to trace the state of origin, it will be even more difficult to figure out whether the attacks were really committed by state officials or by individuals – angry teenagers, 'hacktivists', or cybercriminals, for example.[91] This problem links back to a different debate on the use of force in international law: the question of attribution. According to the famous *Nicaragua* decision of the ICJ, it would be necessary to show 'effective control' of the state over individuals in order to attribute the attack to the state itself.[92] The discussion about attribution stretches from this strict *Nicaragua* requirement on the one side to US President Bush's infamous words '[w]e will make no distinction between the terrorists who committed these acts and those who harbor them'[93] on the other. Most importantly, the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia loosened the *Nicaragua* test slightly by changing 'effective control' to 'overall control',

---

[86] Dröge (n 5) 486.
[87] David Clark and Susan Landau, 'The Problem Isn't Attribution; It's Multi-Stage Attacks', *Proceedings of the Re-Architecting the Internet Workshop* (2010) http://ecir.mit.edu/images/stories/Clark_Landau -Problem isn't Attribution.pdf, 3 (accessed 2 August 2016).
[88] See section 5.1.
[89] Roscini (n 5) 4 et seq.
[90] Clark and Landau (n 87) 3.
[91] Zielowski (n 6) 205.
[92] *Nicaragua* (merits) (n 8) para 109.
[93] George W Bush, 'Address to the Nation on the September 11 Attacks', *Selected Speeches of George W Bush* (11 September 2001) https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf, 58 (accessed 8 September 2016).

a test which would include 'participation in planning and supervision of military operations',[94] but did not manage to convince the ICJ of this standard.[95] Discussing this in too much detail would go beyond the scope of this article, but in most cases it would be difficult to establish evidence for either effective or overall control of the state over a so-called patriotic hacker. The 'harbouring' test by former President Bush is already difficult to justify when it comes to terrorists with significant infrastructure (training camps, weapons etc),[96] and certainly loses any argumentative force when 'harbouring' means that someone is living in the territory of a state and uses a laptop and a connection to the internet. According to the majority of the authors, 'harbouring' needs to be coupled with other acts of 'substantial support',[97] but this does not in any way make the issue of attribution easier or less prone to abuse.

Rid and Buchanan write that 'attribution is what states make of it'.[98] There might be traces of evidence that can lead to certain perpetrators or certain states, but this analysis can suffer from perception bias.[99] The detection of sources is often based on circumstantial evidence like the language or slang term used in source code,[100] the geopolitical context,[101] or, as in the case of Stuxnet, the sophistication and likely cost of the malware used.[102] Even advocates of a robust right to self-defence against cyber-attacks admit that 'technical attribution … can never be absolutely exact'.[103] According to Singer and Friedman, the issue of attribution is 'perhaps the most difficult problem' in this complex.[104]

Tsagourias therefore proposes that 'intelligence and information analysis' need to be used in addition to technical attribution.[105] This, however, is a dangerous path. One only needs to recall the role that biased informers and unreliable intelligence played in the justification of the 2003 Iraq War.[106] Intelligence information is by its very nature secret and impossible to scrutinise externally. Claims that unspecified sources have revealed that an attack was orchestrated by a foreign government are as unreliable as the technical attribution methods.

---

[94] *Tadić* (judgment of 15 July 1999) [1999] ICTY (appeals chamber), paras 120, 145.
[95] *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v Serbia and Montenegro*) [2007] ICJ Rep 43.
[96] Nico Schrijver, 'Responding to International Terrorism: Moving the Frontiers of International Law for "Enduring Freedom"?' (2001) 48 *Netherlands International Law Review* 271, 286.
[97] *Tallinn Manual 2.0* (n 10) 332.
[98] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2015) 38 *The Journal of Strategic Studies* 4, 7.
[99] *Ibid*, 14.
[100] *Ibid*, 19 et seq.
[101] *Ibid*, 23. See also Remus (n 5) 185.
[102] Rid and Buchanan (n 98) 21.
[103] Tsagourias (n 5) 234.
[104] Singer and Friedman (n 5) 73.
[105] Tsagourias (n 5) 234.
[106] See, e.g. Martin Chulov and Helen Pidd, 'Curveball: How US was Duped by Iraqi Fantasist Looking to Topple Saddam', *The Guardian* (15 February 2011) www.theguardian.com/world/2011/feb/15/curveball-iraqi-fantasist-cia-saddam (accessed 25 August 2016).

The danger of the effects doctrine becomes even clearer when looking at a more radical position: Jensen proposes that a state should be allowed to strike back even before the identity of the attacker is proven.[107] Ultimately, he argues, these attacks are so dangerous that and instantaneous that the attribution of an attack would be 'a luxury unavailable in the cyber attack era'.[108] Schmitt argues in a similar vein when he writes about anticipatory self-defence against potential cyber-attacks: 'International law does not require either certainty or absolute precision in anticipating another state's (or non-state actor's) future actions' – 'reasonableness' should be enough.[109] If a state does not even have to fully explore where a cyber-attack comes from, but can defend itself on hunches and suspicions, the door to abuse is wide open.

Neither Article 2(4) nor Article 51 of the Charter are very specific when it comes to the question of how much evidence is required to establish a use of force or an armed attack, but when interpreting a treaty, Article 31 of the Vienna Convention on the Law of Treaties asks us to interpret a provision 'in the light of its object and purpose'. Therefore, it is important to remind ourselves of the founding principles of the United Nations and, most importantly, of the Charter's commitment in its preamble to 'to save succeeding generations from the scourge of war'. The very restrictive framework on the use of force is an integral part of this commitment, and allowing states to use military power based on the suspicion that something *might have* been caused by another state would be the opposite of this.

4.2. Difficulty in detecting the intention of the attack

It is not only difficult to detect the perpetrator of an attack, but also the intention of an attack. Again, the overlap with espionage, described in section 3.2, proves problematic. A cyber-attack uses a similar *modus operandus* to espionage and cybercrime.[110] In all these cases, the most important part of the operation is to gain access to the other system. Failed attempts to do so would not appear different in most cases, and it is not unlikely that an exploitation attempt gone wrong could cause events that get interpreted as a cyber-attack.

Again, Jensen believes that, given the danger and the imminence of cyber-attacks, attempting to find out the intent of the operation is too much to ask for, and the victim state should immediately have the right to self-defence.[111] There is nothing in Article 2(4) or Article 51 that requires intent. Strictly speaking, a rocket fired by accident can constitute a use of force or an armed attack. However, the risk of accidents is much lower when it comes to conventional attacks. When it comes to the

---

[107] Jensen (n 2) 235.
[108] *Ibid*, 232.
[109] Schmitt 'Cyber Operations and the *Jus ad Bellum* Revisited' (n 5) 595.
[110] Brown and Poellet (n 5) 136; Lin (n 5) 82.
[111] Jensen (n 2) 236.

computing world, a much wider range of failed espionage or cybercrime attempts could result in military force being used. Similar to the discussion in the previous subsection, Jensen's positions as well as the more moderate opinions ignoring the intent of a cyber-attack would lead to a dangerous situation that is going against the object and purpose of the UN Charter.

5. The over-hyped nature of the discussion

In addition to examining the legal aspects of the cyber-attack phenomenon, it is also important to consider whether expanding the *jus ad bellum* framework is really as necessary as the authors of the Tallinn Manual and other writers make it out to be.

5.1. Estonia

One of the standing tropes of the cyber-genre is to start any discussion with reference to the Distributed Denial of Service (DDoS) attacks launched against Estonia in 2007. Even though many writers state that these incidents do not constitute a use of force (or an armed attack) under the effects doctrine,[112] a lot of articles use the Estonian attacks as the starting point for their discussions or list them amongst the dangers that cyberwar can/will pose in the future.[113]

In 2007, the already difficult relations between Russia and Estonia, and between Estonia and its significant Russian minority, became even more strained when the Estonian government decided to move the statue of a bronze Soviet Soldier to a less prominent location.[114] This decision led to protests and riots by ethnic Russians within Estonia, who see the statue as a symbol of their wartime sacrifice.[115] Shortly after this decision, the websites of a large number of Estonian institutions, including government ministries, banks, newspapers or political parties, came under attack, and were, as a result, inaccessible for multiple days,[116] a hard blow for a strongly digitalised state like Estonia.[117]

Understandably, Estonian officials were very concerned about the scale of cyber-attacks launched against their state's digital infrastructure: the Minister of Defence stated that these attacks were 'the first time that a botnet threatened the national security of an entire nation',[118] and the

---

[112] See Tsagourias (n 5) 232.
[113] See, e.g. Woltag (n 21) para 1; Roscini (n 5) 4; Brown and Poellet (n 5) 130; Zielowski (n 6) 203; Hoisington (n 5) 443; Schaap (n) 123; Shackleford (n 5) 203.
[114] Ian Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian* (17 May 2002) www.theguardian.com/world/2007/may/17/topstories3.russia (accessed 24 August 2016).
[115] 'Estonia and Russia: A Cyber-Riot', *The Economist* (10 May 2007) www.economist.com/node/9163598 (accessed 24 August 2016).
[116] Traynor (n 114).
[117] 'Estonia and Russia: A Cyber-Riot' (n 115). On the role of the internet in Estonia, see Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence (2010) https://ccdcoe.org/publications/books/legalconsiderations.pdfh, 16 et seq. (accessed 29 August 2016).
[118] Quoted in Davis (n 83).

Speaker of the Estonian Parliament even compared the attacks to nuclear explosions, stating she saw them as 'the same thing', because, '[l]ike nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything'.[119] The spokesperson for the Estonian Ministry of Defence considered the country 'lucky to survive this'.[120]

NATO itself, despite its leaders dismissing the label of 'war' being applied to the attacks,[121] released a video that feeds into the notion of cyberwarfare. The video is full of cuts to experts, footage of uniformed soldiers sitting at computer screens, clips of everyday life in the streets that slowly get darker to dramatic music, and is called 'War in Cyberspace'.[122] While, besides the title, the video makes no mention of the word 'war' itself or of the alleged culprit – Russia – the message is clear: 'there is a real threat to people's security',[123] 'the effects could be devastating',[124] and 'it's absolutely essential that we employ collective defence'.[125]

It is, however, less than clear that it really was the Russian government that was behind these attacks. To date, most evidence seems to suggest that it was, instead, 'hacktivists', unorganised groups of people acting out of their own initiative, as the Tallinn Manual itself states.[126] The only person arrested for the act was a 22 year old Russian living in Estonia who was enraged about the decision to move the statue.[127] If he was even more angry and had used explosives to vent this anger, we would be talking about a terrorist attack, and it is difficult to imagine that NATO would get involved to confront Russia in such a public way.

Even if it the Russian government was clearly behind them, the reality of the attacks is less dramatic than suggested. A DDoS attack is not in any form comparable to a military attack in the way that the NATO video or the statements set out earlier in this section suggest. Generally, DDoS attacks are done by accessing a website or internet service from as many devices as possible, so that the webserver collapses under the amount of traffic. Often, attackers use botnets to commit these attacks – large amounts of previously compromised computers or devices that can be rented on the black market for a variety of purposes like these attacks or sending spam emails. The ever growing market

---

[119] Quoted in *ibid*.
[120] Quoted in Traynor (n 114).
[121] Singer and Friedman (n 5) 122.
[122] NATO, 'Six Colours: War in Cyberspace' (2009) www.youtube.com/watch?v=oGZkCdpPLBE (accessed 9 July 2015).
[123] As the caption at minute 2:09 of the video suggests, shortening a quote from Estonian Defence Minister Jaak Aaviksoo, *ibid*.
[124] Ian West, the Director of NATO's Computer Incident Response Capability Technical Centre, at minute 5:11 of the video, *ibid*.
[125] *Ibid*, at minute 7:53.
[126] *Tallinn Manual 2.0* (n 10) 382.
[127] Bruce Schneier, 'The Cyberwar Threat has been Grossly Exaggerated', *Intelligence Squared US Podcast* (8 June 2010) transcript at http://intelligencesquaredus.org/images/debates/past/transcripts/cyber-war.pdf (accessed 22 August 2015).

for poorly secured connected devices like smart fridges, digital weather stations or cheap routers makes sure that there is a wide range of potentially attacking machines available.[128]

While attacks against Estonian government services in this way are worrying and problematic, they are very different from kinetic attacks. The well-known computer security expert Bruce Schneier stated in a debate that 'it's kind of like the army marches into your country and then gets in line at the motor vehicle bureau so you can't get your driver's license renewed'.[129] Singer and Friedman compare it to bullying rather than to an act of war,[130] and Benatar describes the attacks as 'relatively primitive'.[131]

With the exception of few authors, including Schmitt himself, who argues that the events 'arguably reached the use-of-force threshold',[132] many proponents of the effects doctrine agree that applying this doctrine will not lead to the assessment of these attacks as an armed attack or even a use of force.[133] The statements given by politicians and the video from NATO show, however, how blurry the lines are in the eyes of decision makers. This is not helped by Shackleford's assertion that this event could have led to legitimate self-defence 'if the cyber attack succeeded in bringing the entire country to a halt, capsizing the economy, and unleashing widespread unrests, riots, and possibly deaths'.[134]

It is important to recall that the actual effects of the attack were the temporary unavailability of a range of important websites. Nothing in the events suggests that damage occurred that was even remotely close to 'bringing the entire country to a halt' or to nuclear attacks as suggested by the Estonian government. The events caused an inconvenience and certainly should have been investigated from a criminal law perspective (as, indeed, they were), but they should not be considered as falling within the *jus ad bellum* framework of the United Nations. Nor should they serve as an excuse for expanding this framework.

5.2. Stuxnet

The situation is slightly different in the case of the Stuxnet worm. If the reports are true (and for the purpose of this article, this will be assumed), the United States and Israel managed to cause actual physical damage to the nuclear enrichment programme of Iran. A historic incident with a similar goal

---

[128] Kim Zetter, 'Hacker Lexicon: What are DOS and DDOS Attacks?' *Wired* (16 January 2016) www.wired.com/2016/01/hacker-lexicon-what -are-dos-and-ddos-attacks/ (accessed 4 May 2017).
[129] Schneier (n 127).
[130] Singer and Friedman (n 5) 122.
[131] Benatar (n 5) 375.
[132] Schmitt, 'Cyber Operations and the *Jus ad Bellum* Revisited' (n 5) 577.
[133] Singer and Friedman (n 5) 122; Buchan (n 5) 188; Shackleford (n 5) 239.
[134] *Ibid*, 239.

in the past – the bombing of the Osirak reactor in Iraq by Israeli forces in 1981 – famously was condemned by the Security Council.[135]

Stuxnet caused damage to the Iranian nuclear enrichment programme by manipulating the centrifuges via a worm (the standalone version of a computer virus). This highly sophisticated piece of software spread out by infiltrating Microsoft Windows machines first without causing any harm (in 2010, an estimated 100,000 machines were infected, the vast majority of them in Iran).[136] Once it reached its target network, either accidentally or by deliberate infection through an insider, it tried to spread out via the local network or via USB storage media.[137] On controlling units of certain Siemens centrifuges, the worm attempted to connect to a command-and-control-server over the internet or, on non-connected systems, executed its malicious code without looking for further instructions.[138]

Besides spying on the nuclear programme, the worm caused the centrifuges to run at a higher speed than foreseen for extended periods of time, causing the machines to wear out and break, all while appearing perfectly normal on the control terminals.[139] The exact damage is unknown, as the Iranian government has never disclosed exact numbers (President Ahmadinejad spoke about a 'limited number of centrifuges' that had problems), but it is fairly certain that the Iranian nuclear programme was set back significantly.[140] It is notable that Reuters has quoted a 'U.S. intelligence source' that a similar attack has been attempted, targeting the North Korean nuclear programme.[141]

Besides being a clear case with actual physical damage, Stuxnet is also a rare example that can be relatively well traced to its origins, primarily based on the efforts used: the worm used four very costly zero day exploits (undiscovered security holes in software),[142] and it is likely that its developers had access to the specific types of centrifuges used.[143] It is unrealistic to assume that hacktivist groups or even most governments would have these capabilities.[144] There are also reports

---

[135] UNSC Res 487, UN Doc S/RES/487 (19 June 1981).
[136] Nicholas Falliere, Liam O'Murchu and Eric Chien, 'W.32 Stuxnet Dossier', *Symantec Security Response* (February 2011) www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf (accessed 26 August 2016) 5.
[137] *Ibid*, 3.
[138] *Ibid*, 20.
[139] Michael B Kelley, 'The Stuxnet Attack on Iran's Nuclear Plant Was Far More Dangerous Than Previously Thought', *Business Insider* (20 November 2013) www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T (accessed 27 August 2016).
[140] David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?', *Institute for Science and International Security* (22 December 2010) http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/ (accessed 27 August 2016).
[141] Joseph Menn, 'Exclusive: U.S. tried Stuxnet-Style Campaign against North Korea but Failed – Sources', *Reuters* (29 May 2015) www.reuters.com/article/us-usa-northkorea-stuxnet-idUSKBN0OE2DM20150529 (accessed 26 August 2016).
[142] David Kushner, 'The Real Story of Stuxnet: How Kapersky Labs Tracked Down the Malware that Stymied Iran's Nuclear-Fuel Enrichment Program', *IEEE Spectrum* (26 February 2013) http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (accessed 26 August 2016).
[143] Rid and Buchanan (n 93) 21.
[144] *Ibid*, 22.

relying on anonymous government sources that confirm the widely held suspicions that the governments of the United States and Israel worked on this programme together,[145] and there are a number of other indicators – a refusal to deny US involvement, suspicious smiles at press conferences and a video celebrating the Stuxnet success at the retirement party of an Israeli General, for example, that point towards these two states.[146]

Because of the physical damage that was caused, some academics have concluded that the Stuxnet attacks constitute a violation of Article 2(4) UNC.[147] Depending on which school of thought is followed, the effects could also be interpreted as being grave enough to constitute an armed attack, giving Iran the right to self-defence. Others, however, disagree, stating that the scale of the attack is not sufficient to constitute an armed attack.[148]

Brown and Poellet make the comparison inherent in the effects doctrine and state that '[i]f the damage caused by the Stuxnet malware had instead been caused by a traditional kinetic attack, such as a cruise missile, it is likely Iran would have vigorously responded'.[149] While this is true (if a vigorous response consists of less than starting military strikes against the United States), we can easily make a different analogy: if the same effect had been caused by an American spy or a bribed/persuaded Iranian, who worked covertly in Natanz and manipulated the centrifuge speeds, we would not discuss a war scenario. In fact, this scenario fits the actual events much better – a bombing of the Natanz facility would have very likely resulted in destroyed buildings and human casualties, not just in broken engines of centrifuges.

Stuxnet, therefore, needs to be seen as a case of espionage and sabotage that would be below the *de minimis* threshold usually assumed by states, even below the less strict standard summarised in the espionage debate considered in subsection 3.2, as speeding up centrifuges cannot be construed as 'projecting lethal force'.[150] If the accusations are true, the United States and Israel certainly violated the principle of non-intervention, but, as explained previously, espionage is not caught by international law on the use of force.

5.3. Other scenarios

A lot of articles are very clear about the future: as bad as the attacks that have thus far occurred, such as those discussed in this section, are, we have not experienced the really bad consequences of cyber-

---

[145] Ellen Nakashima and Joby Warrick, 'Stuxnet was Work of U.S. and Israeli Experts, Officials Say', *The Washington Post* (2 June 2012) www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (accessed 26 August 2016).
[146] Richmond (n 6) 855 et seq.
[147] Buchan (n 5), 221.
[148] Roscini (n 5) 76.
[149] Brown and Poellet (n 5) 132.
[150] Ruys (n 72) 160.

attacks yet. The list of potential threats in various academic and journalistic articles reads like a dystopian science fiction novel. Typical narratives are that attackers can

- interrupt the electricity supply[151]
- interrupt communication lines[152]
- derail trains[153]
- steer airplanes off course,[154] or crash them[155]
- cause floods by opening a dam[156]
- damage a state's financial system and cause harm to its economy[157]
- manipulate food and pharmaceutical products at production[158]
- tamper with military communications or weapon systems[159]
- and, as the ultimate threat scenario, cause a meltdown in a nuclear power plant.[160]

Similar scenarios have been raised by former US Secretary of Defense Leon Panetta, who warns of a 'cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability'.[161]

All of this sounds very scary and very real. If a foreign government blows up a nuclear power plant on the press of a button, killing millions of people, the urge to use all necessary means, including military power for self-defence is certainly understandable.

However, it is less than clear that these scenarios are really as realistic as portrayed. Erik Gartzke, for example, has questioned the assumption that cyber doomsday scenarios are likely to occur. He has written that such envisaged scenarios are generally based on the 'common fallacy in arguing from opportunity to outcome, rather than considering whether something that could happen

---

[151] Roscini (n 5) 2; Brown and Poellet (n 5) 135; Christian Whiton, 'Four Steps Obama Must Take to Prevent a Cyber Pearl Harbour', *Fox News* (6 March 2013) www.foxnews.com/opinion/2013/03/06/four-steps-obama-must-take-to-prevent-cyber-pearl-harbor.html (accessed 30 June 2015); Hoisington (n 5) 440.
[152] *Ibid*; Whiton (n 146); Roscini (n 5) 2.
[153] *Ibid*; Boer (n 5) 9; Zielowski (n 6) 203; Nguyen (n 5) 1110.
[154] Boer (n 5) 9.
[155] Roscini (n 5) 2; Zielowski (n 6) 203; Tsagourias (n 5) 229.
[156] Brown (n 5) 187.
[157] Roscini (n 5) 2; Vida M Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 *Naval Law Review* 132, 145 et seq; Buchan (n 5) 213.
[158] Nguyen (n 5) 1110.
[159] Buchan (n 5) 213; Whiton (n 146); Roscini (n 5) 2.
[160] *Ibid*; Brown (n 5) 187; Zielowski (n 6) 203.
[161] Elisabeth Bumiller and Thom Shanker, 'Panetta Warns of Dire Threat of Cyberattack on U.S.', *New York Times* (11 October 2012) www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html (accessed 8 September 2016).

is at all likely, given the motives of those who are able to act'.[162] Unless it comes as part of a general military attack, there are few strategic advantages that a cyber-attack would bring to the attacker.[163] It is also very difficult to use cyber-attacks as a form of threat or blackmail: most attacks are so difficult to execute that the threats would not be taken seriously unless the attacker reveals details – which would then make it easier to prevent the attack.[164]

As pointed out in section 3 above, the cyber-attack scenarios are also not as new as suggested. Traditional espionage and sabotage can achieve most of the damages portrayed, and it can usually do so in a much more realistic and less costly way.[165] A state's train system, for example, will rarely have all its control units connected to the internet, and it will take a lot of insight and highly complex and costly malware to interfere with it. If the goal of an aggressor state is really to derail a passenger train, it would be much easier for it to send a spy to place a hidden obstacle on the tracks – the absence of such attacks in the past demonstrates that the danger of derailing trains due to cyber-attacks is not as overwhelming as many of the articles on the topic suggest.

A more realistic scenario is that cyber-attacks are used as part of normal warfare – the so-called 'hybrid war'. It has been asserted, for example, that Israel used cyber-attacks to disable Syrian air defence before the bombing of Syrian nuclear enrichment facilities,[166] and that Russia's attack on Georgia in 2008 has been accompanied by cyber operations.[167] In neither of these cases, however, would it be necessary to investigate the cyber-attacks further in order to establish if there have been violations of the prohibition of the use of force – they are both clear cases of the use of force (and of armed attacks) even without the launch of worms, viruses or other malware. This kind of hybrid warfare is also by no means a new scenario – it is not that dissimilar from the warriors that, according to legend, circumvented the Trojan defence system by hiding inside a wooden horse.

Another scenario that is usually mixed into this debate, even though it is not a traditional military issue, is the theft of intellectual property and of government data. The US Department of Defence describes in its 'Cyber Strategy' at length how foreign states (especially China) can use cyber-attacks to steal intellectual property.[168] There also have been a lot of reports about Chinese hacking on American government institutions in recent years. Newspapers and academics alike have

---

[162] Erik Gartzke, 'The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth' (2013) 38(2) *International Security* 41, 42.
[163] *Ibid*, 43.
[164] *Ibid*, 59.
[165] Thomas Rid, 'Cyber War Will Not Take Place' (2012) 35(1) *The Journal of Strategic Studies* 5, 28.
[166] Singer and Friedman (n 5) 127; Roscini (n 5) 107.
[167] Brown and Poellet (n 5) 132; Woltag (n 21) para 1.
[168] US Department of Defense, *The DoD Cyber Strategy* (April 2015) www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed 20 July 2015).

written about the Chinese Army breaking into computers of American military, government or industry,[169] or about cyberwar capabilities being developed by the Chinese state.[170]

When Chinese hackers allegedly stole American personnel files in 2015, journalists and government officials even used the Pearl Harbour comparison that has become a bit of a meme,[171] and a relatively moderate Republican Presidential candidate went on record stating that 'China must pay a price' for these incidents and the regular theft of intellectual property.[172]

Similarly, the incidents surrounding Sony Pictures in November 2014 show the danger of the hype and how quickly government agencies can jump to blame states. When Sony Pictures was hacked and embarrassing emails of network executives were leaked, the FBI was quick to link the incidents to the North Korean government, especially since a group claiming to be the hackers threatened cinemas with bomb attacks should they show the film 'The Interview', an otherwise quite irrelevant comedy film mocking Kim Jong-Un.[173] The problems with digital evidence described in subsection 4.1 are certainly true in this case as well. Security experts have criticised the 'Trust Us' mentality displayed by the FBI and the quick jump to conclusions based on circumstantial evidence.[174] Independent analyses of the incidents disagree with the FBI and state that it is more likely the incidents were committed by 'insiders pretending to be North Korea'.[175] Nonetheless, the FBI was quick to state that the incident 'reaffirms that cyber threats pose one of the gravest national security dangers to the United States', and President Obama felt that it was necessary to point out that '[w]e will respond, we will respond proportionally, and in a place and time that we choose'.[176]

Regardless of whether we believe the FBI's claims or not, ultimately we are talking about leaked emails between corporate executives and, in some cases, actors, which proved to be

---

[169] Nguyen (n 5) 1081; Hoisington (n 5) 443.
[170] *Ibid*, 444.
[171] Jonah Goldberg, 'Why are we Ignoring a Cyber Pearl Harbour?', *LA Times* (16 June 2015) www.latimes.com/opinion/op-ed/la-oe-0616-goldberg-china-cyber-hack-20150616-column.html (accessed 30 June 2015); Glenn Harlan Reynolds, 'What if Pearl Harbour Happened and Nobody Noticed?', *USA Today* (14 June 2015) www.usatoday.com/story/opinion/2015/06/14/federal-records-hack-china-pearl-harbor-column/71210018/ (accessed 30 June 2015) (albeit admitting that the label is 'perhaps … a bit strong').
[172] O Kay Henderson, 'Graham warns U.S. in Danger of "Cyber Pearl Harbour"', *Radio Iowa* (5 June 2015) www.radioiowa.com/2015/06/05/graham-warns-u-s-in-danger-of-cyber-pearl-harbor/ (accessed 30 June 2015).
[173] Alex Altman and Zeke J Miller, 'FBI Accuses North Korea in Sony Hacks', *Time* (19 December 2014) http://time.com/3642161/sony-hack-north-korea-the-interview-fbi/ (accessed 31 October 2016); Alex Hern, 'FBI Doubles Down on North Korea Accusations for Sony Pictures Hack', *The Guardian* (8 January 2015) www.theguardian.com/technology/2015/jan/08/fbi-north-korea-accusation-sony-pictures-hack (accessed 31 October 2016).
[174] Bruce Schneier, 'The Government Must Show Us the Evidence That North Korea Attacked Sony', *Time* (5 January 2015) http://time.com/3653625/sony-hack-obama-sanctions-north-korea/ (accessed 31 October 2016).
[175] 'New Clues in Sony Hack Point to Insiders, Away From DPRK', *Security Ledger* (28 December 2014) https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk/ (accessed 31 October 2016).
[176] Oliver Laughland and Dominic Rushe, 'Sony Pulling The Interview was "a Mistake" Says Obama', *The Guardian* (20 December 2014) www.theguardian.com/us-news/2014/dec/19/obama-sony-the-interview-mistake-north-korea (accessed 31 October 2016).

embarrassing for Sony and the individuals concerned, and about vague bomb threats that never materialised. Claiming that this is in the category of the 'gravest national security dangers to the United States' and threatening a response shows the danger of the cyberwar hype.

6. Conclusion

The previous section has shown that the danger of a cyberwar is greatly overstated. The only attack outside an ongoing armed conflict listed in section 5 that comes even remotely close to the damage that could be caused by a military attack is the Stuxnet worm, and the complexity and amount of resources that went into it show that cyber-attacks of that dimension are not going to be common.[177]

It is obvious that many actors in the area have a strong interest to paint a scary picture: contracts and research grants on cyberwar are a fast growing multi-million dollar industry, and the scarier everything looks, the more tax money is channelled into this industry. Journalists already warned about the 'cyber industrial complex' (or variations thereof),[178] and describe an industry that is valued between 80 and 150 billion dollars annually.[179] Newspapers need to be sold, and a headline that states 'Individuals of Russian descend make Estonian servers inaccessible for a few days' is not as helpful for that as 'Russia attacks NATO country in cyberspace', and 'Companies need to improve network security to prevent data theft' is not as exciting as 'Cyber Pearl Harbour: are our nuclear power plants next?'. And governments seek ways to control the internet. The fear of foreign governments that try to attack our nuclear power plants over invisible channels is a fantastic way to justify that it is necessary to 're-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable', as the former US Director of National Intelligence demanded.[180]

It is important that scholars resist the temptation to join the choir of scandalous headlines, and instead consider the reasons for the relatively strict system of the laws on the use of force. Article 51 UNC in particular is very narrow to make sure it cannot be abused. Opening up Article 51 to a form of attack that is almost impossible to attribute clearly would be a dangerous turn for international law.

---

[177] Rid (n 165) 28.
[178] See Bruce Sterling, 'The Cybersecurity Industrial Complex', *Wired* (1 January 2003) www.wired.com/2003/01/the-cybersecurity-industrial-complex/ (accessed 27 August 2016); Jeff Stone, 'Meet the Cyber-Industrial Complex: Private Contractors May Get $7B Windfall From Pentagon's Cyberwar on ISIS', *International Business Times* (7 March 2016) www.ibtimes.com/meet-cyber-industrial-complex-private-contractors-may-get-7b-windfall-pentagons-2329652 (accessed 27 August 2016).
[179] Ron Deibert and Rafal Rohozinski, 'The New Cyber Military-Industrial Complex', *The Globe and Mail* (28 March 2011) www.theglobeandmail.com/opinion/the-new-cyber-military-industrial-complex/article573990/ (accessed 27 August 2016).
[180] Ryan Singel, 'Cyberwar Hype Intended to Destroy the Open Internet', *Wired* (3 January 2010) www.wired.com/2010/03/cyber-war-hype/ (accessed 8 October 2016).

Allowing states to lead a war based on thin technical evidence, maybe backed up by secret intelligence information, is almost asking for abuse.

The language used is especially worrying. 'Pearl Harbour' refers not only to a major military attack that cost the lives of over 2,000 soldiers, but also to the event that was used to justify the American participation in the Second World War. Threatening with such a scenario implies the readiness for a major war fought based on incidents that are unlikely and nearly impossible to prove sufficiently. Rid rightly criticises the 'alarmist' tone of the debate,[181] and O'Connell is correct when she criticises the militarised nature of the discussion that is often led by academics with ties to the military.[182]

The effects doctrine plays into this hype and carries a high danger of abuse due to its practical problems when it comes to attribution. The Tallinn Manual is becoming an extremely influential document in international law, as the various cyber policies and the statements by politicians set out in this article's introduction show – an influence that is only likely increase with the recent publication of the more extensive 2.0 version. It is important for scholars to resist the urge of taking this seemingly plausible doctrine for granted, and instead point to solutions outside the use of force when looking at cyberwar scenarios.

The framework on the use of force is deliberately narrow and should not be expanded to confront an overstated threat. Issues like the use of economic or political force, espionage operations and damage caused under a certain threshold are rightly kept out of the use of force framework, and it would be not only inconsequential, but also dangerous to apply a different approach for computer network attacks.

For world politics, the approach to this problem should instead be to prevent this kind of attack rather than to seek ways to punish it. Countermeasures and military measures as a deterrent are no replacement for improving computer security.[183] While computer systems can never be entirely secure, it is possible to improve the security of the systems in use, and institutions like NATO or the United Nations could play a major role in this. Given many of the revelations by Edward Snowden about American software companies, it is increasingly obvious that the world needs software solutions and digital infrastructure that it can trust. These solutions will have to be developed by international teams and will have to be open source, so that every government agency and any private party is able to review their security.

For a fraction of the money that is now made available to establish military cyber capabilities worldwide, international organisations could coordinate and sponsor such efforts by paying

[181] Rid (n 165) 29.
[182] O'Connell (n 5) 199 et seq.
[183] *Ibid*, 203.

developers to write or audit software. While there will always be a race between those fixing critical security bugs in software and those exploiting them, efforts like this would contribute more to ending the envisioned cyber threat scenarios than threats of military strikes in response can ever do.