Article

The Prohibition of Cyberterrorism as a Method of Warfare in International Law

Stuart Casey-Maslen
https://orcid.org/0000-0001-5181-4002
University of Pretoria
stuart.maslen@up.ac.za

Brenda Mwale
https://orcid.org/0000-0003-3438-9213
PhD Candidate, University of Pretoria
mwale17@gmail.com

Abstract

There is no doubt that cyber operations can play a significant role in the conduct of warfare. In fact, an ongoing cyber arms race among states and non-state actors evokes fears among some of a looming 'digital Pearl Harbour' or a 'digital 9/11'. Given these fears, there have been calls for the elaboration of a 'Digital Geneva Convention' to protect civilians from the harmful consequences of cyberattacks. In this context, this article focuses on one specific aspect of cyber operations during situations of armed conflict: cyberterrorism as a method of warfare. It examines the extent to which international humanitarian law (IHL), which was primarily designed to govern kinetic means and methods of warfare, applies to cyberterrorism. In so doing, it assesses whether the calls for a 'Digital Geneva Convention' are justified.

Keywords: Acts of violence; armed conflict; cyberattacks; cyberterrorism; international humanitarian law.

South African Yearbook of International Law
https://upjournals.co.za/index.php/SAYIL
Volume 44 | 2019 | #7977 | 23 pages

https://doi.org/10.25159/2521-2583/7977
ISSN 2521-2583 (Online), 0379-8895 (Print)

Introduction

In February 2017, the President of Microsoft Corporation, Brad Smith, called for the elaboration of a 'Digital Geneva Convention' to protect civilians from the negative consequences of cyberattacks.[1] Initially, he was thinking of an instrument that would apply in peacetime, in obvious contradistinction to the overwhelming majority of the provisions in the four 1949 Geneva Conventions that apply in armed conflict.[2] But in a blog post later in 2017, Smith recalled that international humanitarian law (IHL) 'was built in an age when military forces squared off on physical battlefields' and suggested that when combat does not take place on a 'traditional battlefield … some traditional international legal protections may not apply.' Refining his earlier proposal, Smith advocated building on the Fourth Geneva Convention's rules to protect civilians in times of war in order to clarify how existing international law, including IHL, applies to cyberspace.[3]

In assessing whether the Microsoft president was justified in his claims and assertions, this article looks at one specific aspect of cyber operations during situations of armed conflict: cyberterrorism as a method of warfare. In recent times, terrorist groups have threatened to launch a 'digital 9/11' with the obvious goal of spreading terror among their targets. But, so far, these threats have yet to materialise. To a large extent, terrorist groups such as Islamic State, al-Qaeda, and Boko Haram have used cyber space for tactical purposes, including recruitment, financing, propaganda, training, and incitement. Where these groups have managed to launch cyberattacks, the attacks have occurred outside the context of an armed conflict. But cyberattacks could also be

1 Brad Smith, 'The Need for a Digital Geneva Convention' (Transcript of Keynote Address at the RSA Conference, San Francisco, February 2017).

2 According to Article 2 common to the four 1949 Geneva Conventions: '*In addition to the provisions which shall be implemented in peacetime*, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.' *See* Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) (hereinafter, 1949 Geneva Convention I) Art 2. As the 2016 commentary by the International Committee of the Red Cross (ICRC) explains, 'although the Geneva Conventions become fully applicable in situations of armed conflict, States Parties have obligations already in peacetime. In particular, States must adopt and implement legislation to institute penal sanctions for grave breaches and take measures to suppress other violations of the Conventions; they must adopt and implement legislation to prevent misuse and abuse of the emblems; and they must train their armed forces to know and be able to comply with the Conventions and spread knowledge of them as widely as possible among the civilian population.' See ICRC, 'Commentary on Article 2, 1949 Geneva Convention I' (*ICRC* 2016) <https://bit.ly/36oJa4G> accessed 1 June 2020.

3 B Smith, 'We Need to Modernize International Agreements to Create a Safer Digital World' (Microsoft, 10 November 2017) <https://bit.ly/36kHjNZ> accessed 10 June 2020.

conducted during armed conflicts, based on the increased use of the internet for terrorist purposes in peacetime.

Whereas cyberterrorism, in peacetime, is largely considered a criminal act which can be addressed through preventive laws (before a cyberattack) or repressive laws (after-the-fact prosecutions), the context of cyberterrorism significantly differs during an armed conflict. This is because certain cyber operations which might be considered criminal in peacetime could comply with international law applicable to a situation of armed conflict. For instance, a denial-of-service attack against an electricity supply website is an offence in peacetime, but the same act does not necessarily violate IHL if it occurs in the conduct of hostilities. For cyber terror attacks which might occur in the context of an armed conflict, key questions arise about the applicability of IHL as well as the potential risks to the civilian population in such contexts. Thus, it is worth examining, more closely, how IHL applies to cyberterrorism.

While the focus of the analysis in this article is on the applicability of IHL, also addressed briefly are the primary rules of *jus ad bellum*. The article seeks to build on and clarify existing knowledge in this area. Thus, for example, the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare* considers in detail how cyber operations in situations of armed conflict are regulated under international law, including but not limited to IHL.[4] More recently, the International Committee of the Red Cross (ICRC) has published a Position Paper entitled 'International Humanitarian Law and Cyber Operations during Armed Conflicts,' which similarly refers to the *ad bellum* rules in the Charter of the United Nations[5] (UN Charter) while concentrating on IHL.[6]

Both documents are relevant to the discussion that follows, although the ICRC Position Paper only refers to the terroristic use of cyberspace in passing. In its latest 'Challenges' paper, elaborated for the 33rd Conference of the Red Cross and Red Crescent in December 2019, the ICRC highlighted as contemporary challenges to IHL both new technologies of warfare (particularly but not only cyber) and terrorism.[7] The paper noted that whereas IHL does not necessarily prohibit online activities like misinformation, online propaganda, and surveillance, it prohibits 'acts or threats of violence the primary

4 Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) (hereinafter, 2013 Tallinn Manual).

5 Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

6 ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (2019) ICRC Position Paper <https://bit.ly/2TZSYim> accessed 10 June 2020.

7 ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions' (22 November 2019) Document 33IC/19/9.7.

purpose of which is to spread terror among the civilian population.'[8] Although the paper did not explicitly mention cyberterrorism, it referred to the prohibition against 'spreading terror' in the context of other cyber operations.

It is in this context that this article examines the extent to which cyberterrorism is prohibited as a method of warfare under IHL. This article first provides a general overview of the role of cyber operations in warfare, setting the scene for further discussion on cyberterrorism. After this preliminary discussion, the article examines the applicability of IHL to cyberterrorism. In so doing, it assesses whether cyberattacks qualify as 'acts of violence' as understood in IHL and analyses the extent to which such acts of violence can provoke terror. The article briefly looks at the rules of *jus ad bellum* and concludes by discussing whether there is a need for a 'Digital Geneva Convention' based on the applicability of existing IHL.

The Role of Cyber Operations in Warfare

No one doubts the significance of cyber operations to the conduct of warfare. Michael Klare has claimed that, although it is occurring largely in secret, an 'arms race in cyberspace' is underway.[9] And as the ICRC affirms, while very few states have admitted to using cyber operations, a growing number are building their cyber capabilities, and their use, the organisation believes, 'is likely to increase in future.'[10] Klare's primary concern was one of escalation through cyber operations between military powers in conflict, 'eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict.'[11] But he also signalled the threat of terrorist organisations seeking to provoke a global nuclear crisis 'by causing early-warning systems to generate false readings ('spoofings') of missile launches.'[12]

To date, the most significant use of cyber operations to cause physical damage is probably the Stuxnet worm, a form of malware seemingly developed by the United States and Israel with a view to damaging centrifuges at the Iranian uranium enrichment facilities at Natanz, in an operation codenamed 'Olympic Games'.[13] The Iranian centrifuges in question were said to normally spin at 1,064Hz, but the resultant virus caused the rotors inside to slow to a frequency of several hundred hertz for 50 minutes.

---

8 ICRC (n 7) 29.

9 Michael T Klare, 'Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation' (*Arms Control Today* November 2019) <https://bit.ly/2USw1gk> accessed 16 June 2020.

10 ICRC (n 6) 3.

11 Klare (n 9).

12 ibid.

13 David P Fidler, 'Cyberattacks and International Human Rights Law' in Stuart Casey-Maslen (ed), *Weapons under International Human Rights Law* (Cambridge University Press 2014) 303; and see Ralph Langner, 'Cracking Stuxnet, a 21st-Century Cyber Weapon' (*TED*, 29 March 2011) <https://bit.ly/349ErC2> accessed 16 June 2020.

As a result, the aluminium tubes expanded, increasing the chances of collision between different parts of the tubes, thus destroying the centrifuges. Six cascades, each containing 164 centrifuges, were reportedly destroyed in this manner.[14] It is claimed that Iran's centrifuges at Natanz experienced a number of failures in mid- to late 2009, resulting to more than 900 machines being taken out of service by technicians; Stuxnet was identified as the likely cause of the failures.[15]

The *Tallinn Manual* asserts that Stuxnet amounted to a use of force based on the damage caused to the Iranian centrifuges.[16] If so, whether this was lawful under *jus ad bellum*, this would indicate the existence of an armed conflict if the cyberattack rose to the level of an armed attack or was conducted in the course of an ongoing armed conflict.[17] The fact that neither Iran nor the United States characterised the cyber operation as a hostile act amounting to an armed conflict is relevant, but not conclusive. Although a meltdown at the Natanz facility does not seem to have been a likely, or even a possible, outcome in the prevailing circumstances,[18] one could speculate that a different and more serious cyberattack could have been devised to provoke just such an event. Would such an attack, where the facility was not a lawful military objective under IHL, not be characterised as terrorist in nature if its primary aim was to spread terror?

In 2015, the UN Secretary-General noted that among the complex issues that have emerged in recent years is the 'growing malicious use' of information and communications technologies (ICTs) by 'extremists, terrorists and organized criminal groups.'[19] Warnings about the potential for devastating cyberattacks against nuclear power plants in the United States are longstanding, but were reawakened by Stuxnet.[20] Preparations to confront growing cyber threats against nuclear facilities are, though, ongoing worldwide; an exercise drill in October 2017 at a research facility 110 miles south-west of Stockholm is said to have been the most sophisticated cyber exercise to

---

14 Holger Stark, 'Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War' (*Der Spiegel,* 8 August 2011) <https://bit.ly/2uxypPO> accessed 16 June 2020.

15 David Albright, Paul Brannan, and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment' (*Institute for Science and International Security*, 22 December 2010) <https://bit.ly/2RAyk7c> accessed 16 June 2020.

16 Commentary on Rule 10 para 9, 2013, Commentary on Rule 13 para 13, 2013 Tallinn Manual; see also Michael N Schmitt, 'The Use of Cyber Force and International Law' in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) 1127.

17 But for a contrary view, see, eg, David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) J Conflict and Security L 287.

18 See, eg, George Jahn, 'Stuxnet Virus Penetrates Nuclear Plant, May Cause Chernobyl-Like Disaster' *The Christian Science Monitor, Associated Press* (Vienna, 31 January 2011) <https://bit.ly/2sWbcFZ> accessed 16 June 2020.

19 UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174.

20 Charles Ferguson and Frank Settle (eds), 'The Future of Nuclear Power in the United States' (*Federation of American Scientists*, 2012) 74, 77 <https://bit.ly/2PxlBQ7> accessed 16 June 2020.

date in which the International Atomic Energy Agency (IAEA) had participated. After all, 'a cyberattack combined with a physical one could, in theory, lead to the release of radiation or the theft of fissile material.'[21]

Nuclear facilities are certainly not immune from cyber operations. In more recent times, India confirmed in late October 2019 that its newest nuclear power plant, at Kudankulam, had been the victim of a cyberattack. The plant was hacked using a data extraction malware linked to the Lazarus Group.[22] This was not an incident of physical destruction but again emphasised the potential vulnerabilities of nuclear plants. One Indian parliamentarian, Shashi Tharoor, the former UN Under-Secretary-General for Communications and Public Information, asked, 'Why has it taken so long for the government to create and fortify India's cyber capabilities in order to punish, deter and repel such attacks?'[23]

As non-state actors such as 'extremists, terrorist and organized criminal groups' continue to develop their cyber capabilities, attacks such as with Stuxnet and at Kudankulam may no longer be extraordinary. Future cyber operations might increase in severity and play a significant role in warfare. Besides, the effects of such attacks might span borders, affecting nations which were not initially targeted. In this regard, it must be noted that no single state is immune to a cyberattack, even the less technologically developed countries. Given these possibilities, it is vital to analyse the extent to which IHL, which is intended to govern traditional means and methods of warfare, applies to cyberterrorism.

The Regulation of Cyberterrorism as a Method of Warfare under IHL

International law governing cyberterrorism is potentially clearer and less controversial when such acts are conducted as a method of warfare during an armed conflict than when such acts are carried out in peacetime. This is because the definition under IHL is narrower in scope and less politically charged. There is no question, for instance, that both states and armed groups struggling on behalf of a people exercising its right of self-determination may both violate IHL. According to the key IHL rule: 'Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.' This is so, whether the armed conflict is international or non-international in character.[24] Moreover, this is a rule of customary international law

---

21 Sean Lyngaas, 'Hacking Nuclear Systems is the Ultimate Cyber Threat. Are We Prepared? Nightmare Scenario' (*The Verge*, 23 January 2018) < https://bit.ly/34bW2JC> accessed 17 June 2020.

22 Stephanie Findlay and Edward White, 'India Confirms Cyber Attack on Nuclear Power Plant' *Financial Times* (Seoul, 31 October 2019) <https://on.ft.com/37sfPa9> accessed 17 June 2020. The Lazarus Group is said to have ties to two North Korean-backed groups.

23 ibid.

24 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7

applicable to all states, including those that are not parties to the two 1977 Additional Protocols to the four Geneva Conventions of 1949.[25]

Before examining how this key rule of IHL applies to cyberattacks, it is necessary to highlight the two clear differences between this primary IHL rule governing terrorism and corresponding prohibitions on terrorist acts committed in peacetime.[26] First and foremost, to fall within the scope of the IHL prohibition, acts of violence must be directed against civilians or the civilian population more broadly (or at the least be indiscriminate), but not targeted against the military. Contrast that with the 1997 Terrorist Bombings Convention, for instance, according to which a person commits a crime if he or she 'unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility.'[27] The prohibition in the 1997 Terrorist Bombings Convention clearly encompasses—and outlaws—attacks against a military barracks or the Ministry of Defence, both potentially lawful military objectives in the course of an armed conflict under IHL.[28]

Second, the requisite intent in each of the two provisions also differs substantively. In the case of the IHL rule, the primary (though not exclusive) purpose of the acts of violence must be to spread terror among the civilian population. As the ICRC explained in its commentary on the provision in the 1977 Additional Protocol I,

> there is no doubt that acts of violence related to a state of war almost always give rise to some degree of terror among the population and sometimes also among the armed forces. It also happens that attacks on armed forces are purposely conducted brutally in

December 1978) (hereinafter, 1977 Additional Protocol I) Art 51(2); Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978 (hereinafter, 1977 Additional Protocol II) Art 13(2).

25 ICRC, 'Customary IHL Study, Rule 2.Violence Aimed at Spreading Terror among the Civilian Population' <https://bit.ly/2ONFTT7> accessed 10 June 2020; and Prosecutor v Galić (Judgment) IT-98-29-A (30 November 2006) paras 87–89.

26 As the ICRC recalls, as IHL 'applies only during armed conflict, it does not regulate terrorist acts committed in peacetime. Such acts are however subject to law, ie domestic and international law, in particular human rights law.' ICRC, 'What does IHL Say About Terrorism' (ICRC, 22 January 2015) <https://bit.ly/2PxbWsY> accessed 10 June 2020.

27 International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) (hereinafter, 1997 Terrorist Bombings Convention) Art 2(1).

28 1977 Additional Protocol I, Art 52(2). According to the rule, which applies as a matter of custom in all armed conflicts, 'In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.' See ICRC, 'Customary IHL Study, Rule 8. Definition of Military Objectives' <https://bit.ly/2X2mHqu> accessed 11 June 2020.

> order to intimidate the enemy soldiers and persuade them to surrender. This is not the sort of terror envisaged here.[29]

What is envisaged are gratuitous acts that offer no military advantage but are directed against civilians or civilian objects with a view to causing 'extreme fear' among the civilian population.[30] Under the Terrorist Bombings Convention, however, the intent must be to either kill or cause serious bodily injury, or 'to cause extensive destruction of such a place, facility or system, where such destruction results in or is likely to result in major economic loss.'[31] This is clearly of much broader ambit.[32]

The apparent incompatibility between the Terrorist Bombings Convention and IHL is resolved by a dedicated provision in the 1997 Convention. Therein it is stated that the 'activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention.'[33] Thus, acts committed during a situation of armed conflict will only fall within the scope of the Convention if they lack sufficient nexus to be considered acts in the conduct of hostilities.[34] This exclusion is generally understood to encompass acts in the conduct of hostilities by both state and non-state armed groups that are party to an armed conflict.[35] A similar exclusion was incorporated in the 2005 draft of the Comprehensive Convention on International Terrorism (an instrument still to be concluded and adopted).[36] Having considered the two primary differences between the primary IHL rule governing terrorism and the prohibitions on terrorism in peacetime, this article now turns back to discuss how the key rule of IHL, prohibiting acts or threats of violence aimed at spreading terror, applies to cyberattacks.

---

29 Thus, the significance of this rule lies in the fact that it distinguishes acts primarily aimed at spreading terror from acts or threats of violence in the normal conduct of hostilities, which may be unlawful but that are not carried out with such a primary purpose. See eg, Yves Sandoz, C Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (ICRC/Martinus Nijhoff 1987) para. 1940.

30 *Prosecutor v Galić* (Judgment) IT-98-29-T (5 December 2003) para 137.

31 1997 Terrorist Bombings Convention Art 2(1)(a) and (b).

32 That said, Art 5 of the Convention imposes on each state party the obligation to 'adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention, in particular where they are intended or calculated to provoke a state of terror in the general public or in a group of persons or particular persons.' *See* 1997 Terrorist Bombings Convention Art 5.

33 1997 Terrorist Bombings Convention Art. 19(2).

34 For the precise inter-relationship see Ben Saul, 'Terrorism, Counter-terrorism, and International Humanitarian Law' in Ben Saul and Dapo Akande (eds), *The Oxford Guide to International Humanitarian Law* (OUP 2020) 412.

35 Stuart Casey-Maslen and Steven Haines, *Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict* (Hart 2018) 328.

36 Draft Comprehensive Convention on International Terrorism, in Appendix I to UN Doc A/59/894 of 12 August 2005 Art 20(2).

Are Cyberattacks Acts 'of Violence'?

The first important issue to the application of the primary IHL rule is whether a cyberattack qualifies as an 'act of violence'.[37] There is no definition under IHL of an act of violence, but it is generally understood as meaning the use of physical force leading, or potentially leading to damage to property or harm to a person. While such damage or harm may be the result of a cyberattack, the attack itself does not involve physical force. It can be argued that a weapon, a means of warfare, and a method of warfare should be deemed to encompass cyber operations,[38] but this does not resolve the question of interpretation under IHL of the notion of 'violence'. The Tallinn Manual, however, is unequivocal on this point, affirming that since the term is not limited to activities that release kinetic force—encompassing, it is 'universally agreed', biological, chemical, and radiological attacks—what counts are the 'consequences' of an operation and not its 'nature'.[39] Violence, the experts that contributed to the Tallinn Manual concluded, 'must be considered in the sense of violent consequences, and is not limited to violent acts.'[40] This rather flies in the face of the ordinary meaning of the word, however. There is also a distinction potentially to be drawn between the harm resulting directly from the physical properties of a weapon and the harm that results indirectly from the effects of its use. That said, the Tallinn Manual is a highly influential document and its interpretations carry considerable weight.[41]

The findings of the Manual are also reflected in the view of the ICRC. [42] The ICRC makes reference to Article 49 of Additional Protocol I, which defined the term attack as '*acts of violence* against the adversary, whether in offence or in defence' [emphasis added] and duly affirms that 'the question of how widely or narrowly the notion of "attack" is interpreted with regard to cyber operations is … essential for the applicability of these rules and the protection they afford to civilians and civilian infrastructure.' It asserts that it is 'widely accepted that cyber operations expected to cause death, injury

---

37 Of academic note, under the definition of 'explosive or other lethal device' in Art 1(3) of the 1997 Terrorist Bombings Convention a cyberattack would appear not to qualify as, even if the attack resulted in death or serious injury, it cannot be considered an 'explosive or incendiary weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage.' Nor is it a 'weapon or device that is designed, or has the capability, to cause death, serious bodily injury or substantial material damage through the release, dissemination or impact of toxic chemicals, biological agents or toxins or similar substances or radiation or radioactive material.'

38 See, eg, Stuart Casey-Maslen, *Jus ad Bellum: The Law on Inter-state Use of Force* (Hart 2020) ch 1.

39 Commentary para 3 on Rule 30, 2013 Tallinn Manual.

40 ibid. See further on this issue Michael Schmitt, 'International Humanitarian Law and the Conduct of Hostilities', in Saul and Akande (n 34) 173.

41 Although the Manual is a non-binding document, it has had considerable influence which led to the creation of a Second Tallinn Manual. *See* eg, Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) i; Tobias Kliem, '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' (2017) J on the Use of Force and Intl L 4(2) 5.

42 ICRC (n 6) 5 and *ff*.

or physical damage constitute attacks under IHL.' [43] In the ICRC's view, this includes harm arising from 'the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply.'[44] But the ICRC goes considerably further in its appreciation of the extant law:

> Beyond this, attacks that significantly disrupt essential services without necessarily causing physical damage constitute one of the most important risks for civilians. Diverging views exist, however, on whether a cyber operation that results in a loss of functionality without causing physical damage qualifies as an attack as defined in IHL. In the ICRC's view, during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means.[45]

Given that there are situations where the functionality of a computer system can be simply restored by re-introducing data, this is stretching the notion of an 'act of violence' to its breaking point. Nonetheless, the ICRC argues that if the notion of attack is interpreted as 'only referring to operations that cause death, injury, or physical damage', a 'cyber operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or which is expected to cause such effect incidentally, might not be covered by essential IHL rules protecting the civilian population and civilian objects.' Such an 'overly restrictive understanding of the notion,' the organisation argues, 'would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities.' It concludes that it is 'essential that States find a common understanding in order to adequately protect the civilian population against the effects of cyber operations.'[46] Indeed it is. For if the ICRC's interpretation is correct, a hacker who sends huge quantities of spam to a military account which overwhelms the server and blocks access to the internet could fall within this notion. He or she could be thereby deemed to be participating directly in hostilities, making them a target for lethal force by the adversary.[47] More clarity is, therefore, needed on how IHL applies to such situations.

Acts of Violence that Provoke Terror

The second issue to examine is whether cyberattacks can provoke terror. It must be noted at the outset that acts or threats of violence may be lawful or unlawful in the context of an armed conflict, but violent acts classified under IHL as 'terrorist' are always unlawful. With respect to the application of the rule prohibiting terror attacks more broadly, the ICRC has stated that air raids have frequently been used to terrorise

43 ibid 7.
44 ibid.
45 ibid 7–8.
46 ibid 8.
47 See, eg, Turns (n 17) 286–87; Schmitt (n 40) 173–74.

the population, but it notes that these 'are not the only methods'.[48] However, as Yoram Dinstein points out, large-scale aerial bombardments that are 'pounding' military objectives and 'breaking the back of the enemy armed forces' are not unlawful according to this rule, 'even if they lead … to the collapse of civilian morale.' [49]

In the context of the conflicts in Bosnia and Herzegovina, the so-called Siege of Sarajevo has been held to have included violations of the rule prohibiting terror attacks. In accepting the prosecution's argument against General Galić, the commander of the Bosnian Serb army around Sarajevo in 1992–1994, that the main aim of the army's campaign of sniping and shelling against civilians in the city was to provoke a state of terror, the International Criminal Tribunal for the former Yugoslavia (ICTY) found that the evidence presented demonstrated that the Bosnian Serb army 'attacked civilians, men and women, children and elderly in particular while engaged in typical civilian activities or where expected to be found, in a similar pattern of conduct throughout the city.'[50] In 1993, UN representatives recorded more than 400 artillery and mortar impacts on a single day in the general area of Stari Grad, concluding that there was 'no doubt that civilians in that area were deliberately targeted … because of the unusually high volume of fire there, which would seem to have no military value.' [51]

The underlying principles of these findings were reflected in the Special Court for Sierra Leone's judgment on appeal against conviction by Charles Taylor, the former President of Liberia, for his involvement in the conflict in Sierra Leone in the late 1980s and the 1990s. The Appeals Chamber declared itself satisfied that the RUF (Revolutionary United Front) and AFRC (Armed Forces Revolutionary Council) had conducted acts of terror as the 'primary modus operandi'. The strategy employed extreme fear, but not 'aimless' terror.

> Barbaric, brutal violence was purposefully unleashed against civilians because it made them afraid – afraid that there would only be more unspeakable violence if they continued to resist in any way, continued to stay in their communities or dared to return to their homes. It also made governments and the international community afraid – afraid that unless the RUF/AFRC's demands were met, thousands more killings, mutilations, abductions and rapes of innocent civilians would follow. The conflict in Sierra Leone was bloody because the RUF/AFRC leadership deliberately made it bloody.[52]

---

48 Sandoz and others(n 29) para 4785.

49 Yoram Dinstein *The Conduct of Hostilities Under the Law of International Armed Conflict* (3rd edn, Cambridge University Press 2016) para. 390.

50 *Prosecutor v Galić* (Judgment) ICTY-98-29-T (5 December 2003) para 593.

51 ibid para 435.

52 *Prosecutor v Charles Ghankay Taylor* (Judgment) SCSL-03-01-A (26 September 2013) para 300.

That does not mean, though, that in order to provoke terror, attacks must be sustained and carried out over a protracted period. Thus, in its interpretation of the IHL rule prohibiting terror attacks against civilians (included as Rule 36 in the Tallinn Manual), the Manual suggests that an example of the rule's application to cyber operations would be a cyberattack on a mass transit system causing death or injury where the main objective was to terrorise the civilian population.[53] While hardly an emblematic illustration of the rule, it does serve to confirm that a single attack may be sufficient. This would be especially the case where an attack concerned use of biological or chemical agents, and *a fortiori*, a nuclear weapon. It is also important to recall that 'threats', as well as acts of violence, fall within the customary and conventional prohibition of terror attacks. As the ICRC observed in their commentary on the provision in the 1977 Additional Protocol I, this 'calls to mind some of the proclamations made in the past threatening the annihilation of civilian populations.' [54] Cyber operations could certainly be used to inflict huge suffering on the civilian population; if the Tallinn Manual is correct, a threat to do so would also be encompassed. Thus, therein it is asserted that: 'A threat to use a cyberattack to disable a city's water distribution system to contaminate drinking water and cause death or illness would violate the Rule if made with the primary purpose of spreading terror among the civilian population.' [55]

The Manual holds that while the Rule prohibits only conducting or threatening cyber terror attacks, 'employing cyber means to communicate a threat of kinetic attack with the primary purpose of terrorizing the civilian population is likewise prohibited by the law of armed conflict.'[56] However, there might be situations where a terrorist group carries out a cyberattack without threatening a kinetic attack. Consider, for instance, a denial-of-service attack against a government website which replaces the website with the image of a terror organisation. Here, the cyberattack in itself is not 'violent' and does not communicate a threat of an attack. Thus, based on the Tallinn Manual, such an attack would not violate the primary IHL rule prohibiting terror, even though it might cause fear to those who access the said websites.

The Manual also deliberates over an example of 'a false tweet (Twitter message) sent out to cause panic, falsely indicating that a highly contagious and deadly disease is spreading rapidly throughout the population. Because the tweet is neither an attack nor a threat thereof, it does not violate this Rule.'[57] The ICRC picks up on this issue in its

53 Commentary para 2 on Rule 36, 2013 Tallinn Manual.
54 Sandoz and others(n 29) para 1940.
55 Commentary para 3 on Rule 36, 2013 Tallinn Manual.
56 Commentary para 6 on Rule 36, 2013 Tallinn Manual.
57 Commentary para 3 on Rule 36, 2013 Tallinn Manual.

latest 'Challenges' paper mentioned in the introductory paragraphs, observing that, in recent conflicts,

> certain uses of digital technology other than as means and methods of warfare have led to an increase in activities that adversely affect civilian populations. For example, misinformation and disinformation campaigns, and online propaganda, have fused on social media, leading in some contexts to increased tensions and violence against and between communities.[58]

While, the ICRC acknowledges, IHL 'does not necessarily prohibit such activities,' other bodies of law, it suggests, including international human rights law, 'might also be relevant when assessing surveillance and disinformation.'[59] In any case, not all cyberattacks can provoke terror. The essence of the primary IHL rule prohibiting terrorism is based on the distinction between civilians and civilian objects and military objectives, including combatants. It must, therefore, be noted that the principle does not depend much on the means of the attack (e.g., cyber or kinetic), but rather on the targeting and the expected effects on civilians.

The Regulation of Cyberterrorism under *Jus ad Bellum*

While terrorism has been an issue of international concern for many decades, it shot up the international agenda following the 9/11 attacks against the United States (US) perpetrated by al-Qaeda. In its Resolution 1373, adopted in the aftermath of the attacks, the UN Security Council reaffirmed that 'any act of international terrorism' constitutes a threat to international peace and security.[60] The United States has chosen to prosecute those directly responsible for the 9/11 attacks as war criminals rather than charging them with terrorist offences under US domestic law. This means that they must demonstrate beyond a reasonable doubt that there was an armed conflict between the United States and al-Qaeda on or before 11 September 2001.[61]

The United States did not seek UN Security Council authorisation to use force in its response to the 9/11 attacks—although it would undoubtedly have secured it at the time—choosing to rely instead on its inherent right of self-defence, as codified in Article 51 of the UN Charter. In so doing, it asserted that an 'armed attack' had been carried out against it by a non-state actor, albeit with a degree of complicity of the Taliban regime ruling in Afghanistan where al-Qaeda's leadership were hosted. This flew in the face of the prevailing interpretation of the existing law (including among earlier US

58 ICRC (n 7) 21.

59 ibid.

60 UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373, third preambular para.

61 That al-Qaeda had committed terrorist offences would have been far easier to prove. The attack on the Twin Towers is without a doubt a terror attack. There is no need to prove the existence of an armed conflict. Moreover, the attack against the Pentagon on 9/11 cannot be considered a war crime *per se* as it was a lawful military objective under IHL.

government legal opinion),[62] which held that an armed attack must be the action of a state. The attack may be conducted directly through its armed forces or by the state sending armed groups or mercenaries to do its bidding.[63] Thus, although the Taliban regime provided sanctuary to al-Qaeda, concluding that an 'armed attack' occurred based on this argument is a stretch. If, however, it is true that the law has changed, it is that rarest of occurrences, instantaneous creation or amendment of customary international law.[64]

Before launching its attacks on Afghanistan in October 2001, the United States issued a set of demands to the Taliban ruling regime in Afghanistan requiring, in particular, that the Taliban close al-Qaeda's training camps in Afghanistan and hand over Osama bin Laden for trial.[65] It did not immediately launch a military attack on Afghanistan; to do so would not have complied with the principle of necessity that underpins the exercise of self-defence. Critically, this delay in response also enabled the United States to verify their belief that al-Qaeda was indeed responsible for the 9/11 attacks.[66] The Taliban, however, demanded firm evidence of bin Laden's guilt before they would countenance such a move.[67]

These issues have obvious resonance for cyberterrorism and *jus ad bellum*. If we return to the case of the Stuxnet worm and the uranium enrichment facility at Natanz, while this likely involved an unlawful use of force in violation of Article 2(4) of the UN Charter (a *jus cogens* norm),[68] no state ever claimed responsibility. Had it amounted

---

62 In 1949, the Committee on Foreign Relations of the US Senate declared that 'the words "armed attack" clearly do not mean an incident created by irresponsible groups or individuals, but rather an attack by one state upon another.' US Senate, 'Report of the Committee on Foreign Relations on the North Atlantic Treaty' (6 June 1949) Executive Report No 8; see Ian Brownlie, *International Law and the Use of Force by States* (OUP 1963) 278.

63 Definition of Aggression adopted by UN General Assembly Resolution 3314 (XXIX) (adopted without a vote on 14 December 1974) UN Doc A/RES/3314 (hereinafter 1974 Definition of Aggression) Art 3(g).

64 Michael Byers, 'The Intervention in Afghanistan—2001' in Tom Ruys, Olivier Corten and Alexandra Hofer (eds), *The Use of Force in International Law: A Case-Based Approach* (OUP 2018) pp. 625–38, at 634.

65 See, eg, Daniel DePetris, 'The War in Afghanistan Turns 19 Years Old' (*Washington Examiner,* 10 July 2020) <https://bit.ly/3nHyjv7> accessed 20 August 2020; see also Paul Holtom, 'United Nations Arms Embargoes Their Impact on Arms Flows and Target Behaviour: Case study: The Taliban, 2000–2006' (2007) 4–8 <https://bit.ly/2IWuOlH> accessed 12 November 2020.

66 See, eg, L Wright, *The Looming Tower: Al-Qaeda and the Road to 9/11* (Alfred P. Knopf 2006) 362–367.

67 See, eg, Jeremy Hammond, 'Newly Disclosed Documents Shed More Light on Early Taliban Offers, Pakistan Role' (*Foreign Policy Journal* 20 September 2010) <https://bit.ly/2YaDt5v> accessed 13 June 2020.

68 See, eg, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America*), (Judgment) (Merits), (1986) ICJ Rep 14 para 190, citing para 1 of the commentary of the Commission to Art 50 of the International Law Commission (ILC)'s draft Articles

also to an armed attack (which in the circumstances seems highly unlikely), against which state or states would Iran have been entitled to use force in self-defence?

If we consider a similar, or greater, use of cyber force by an individual belonging to or supporting a non-state actor, the problem of attribution only increases.[69] As noted above, whether or not a non-state actor can indeed commit an armed attack remains in dispute. So, given that the right of self-defence under *jus ad bellum* gives a state the right to use considerable armed force on the territory of another state, being certain about the facts and being certain about the law are two major challenges that are only exacerbated by cyber operations, and especially when non-state actors are involved.

Nonetheless, the fact that a cyber operation was launched by a non-state actor does not, according to the Tallinn Manual, preclude a state from exercising its right of self-defence. [70] But, in terms of attribution, the 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security duly noted that 'the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State', and, moreover, 'accusations of organizing and implementing wrongful acts brought against States should be substantiated.'[71] Similarly, under *jus in bello,* it is understood that '[i]dentifying actors who violate IHL in cyberspace and holding them responsible is likely to remain challenging.'[72] Besides, without proper evidence tracing a certain cyber operation to its source, it is difficult to establish responsibility.

Assuming that Iran identified the actors behind Stuxnet and that the attack rose to the level of an armed attack, the next question would be whether to respond with cyber or kinetic force. This question arose in relation to Israel's response to a cyberattack by Hamas. In perhaps the first publicly known example of retaliation using kinetic force, the Israel Defense Forces (IDF) bombed a building where Hamas cyber operatives worked, claiming that the building was used by Hamas to attack Israel's cyberspace.[73] In this case, however, the cyberattack was carried out in the course of an ongoing armed conflict, potentially justifying Israel's response.

If, however, the cyberattack rose to the level of an armed attack and was an isolated attack taking place outside an armed conflict, would Israel's response be justified? For

on the Law of Treaties. United Nations, *Yearbook of the International Law Commission* (Vol II) (United Nations 1966) 247.

69 UNGA (n 19) para. 7.

70 Commentary para 16 on Rule 13, 2013 Tallinn Manual.

71 UNGA (n 19) para 28(f).

72 ICRC (n 7) 20.

73 Cyber Security Intelligence, 'Israel Responds to a Cyber Attack with Bombs' (*Cyber Security Intelligence* 10 May 2019) <https://bit.ly/39DSzrj> accessed 14 June 2020.

Nils Melzer, a 'self-defence cyber action', must be justified by the seriousness of the harm to be prevented.[74] Andrew Rundle, on the other hand, argues that it does not matter whether the response is cyber or kinetic; what matters is whether the response adheres to the principle of proportionality.[75] In this context, three factors have been proposed for determining whether forceful kinetic responses are justified. First, a cyberattack should be part of an 'overall operation culminating' in armed attack. Second, the attacker should have taken an irrevocable step towards an attack rendering the attack unavoidable. Lastly, the defending state acts in advance of the attack 'during the last possible window of opportunity available to effectively counter the attack.'[76]

While the above factors might serve as a useful guideline for nations acting in defence, identifying how defensive kinetic actions fulfil the customary law requirements for the legality of self-defence, particularly the necessity and proportionality of a forcible response, will remain tricky. In this regard, accurately and swiftly identifying the attacker is of paramount importance. These factors similarly pose a significant obstacle to the proper application of IHL.

Concluding Remarks

Was the President of Microsoft justified in his call for the elaboration of a 'Digital Geneva Convention' to address cyber operations as a method of warfare? Considering the unique nature of cyber operations, there are good reasons to think that he was. Whereas it has been established that 'acts of violence' can be carried out by cyber means and that it is the 'consequences' and not the 'violent nature' of the acts that should be considered, there the consequences of a cyber operation are purely digital or non-destructive. In such situations, one can conclude that IHL does not anticipate 'acts of terror' in the context of the cyber space.

Speaking before the UN Security Council in September 2019, the UN Secretary-General made the following observations:

> We face an unprecedented threat from intolerance, violent extremism and terrorism. It affects every country, exacerbating conflicts and destabilizing entire regions, and it is constantly evolving. The new frontier is cyberterrorism: the use of social media and the dark web to coordinate attacks, spread propaganda and recruit new followers.[77]

---

74 Nils Melzer, 'Cyberwarfare and International Law' (*United Nations Institute for Disarmament Research* 2011) 18 <https://bit.ly/2STRiqg> accessed 14 June 2020.

75 Andrew Rundle, 'International Acceptance of Kinetic Operations in Response to a Cyber Attack' (Master's Thesis, Marine Corps University 2011) 19.

76 Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' [1999] 37(3) Columbia J Transnatl L 932–933.

77 UN, 'Secretary-General Calls Cyberterrorism using Social Media, Dark Web, 'New Frontier' in Security Council Ministerial Debate' (25 September 2019) UN Doc SG/SM/19768-SC/13964.

But while cyberspace 'touches every aspect of our lives', making cyberspace stable and secure 'can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.'[78] Yet, despite the elaboration of the Tallinn Manual, applicable international law remains uncertain.

For the ICRC, 'there is no question that IHL applies to, and therefore limits, cyber operations during armed conflict.'[79] It acknowledges, however, that states may 'decide to impose additional limits to those found in existing law and develop complementary rules, in particular in order to strengthen the protection of civilians and civilian infrastructure against the effects of cyber operation[s].'[80] The ICRC believes that new rules 'need to build on and strengthen the existing legal framework, including IHL.'[81] Thus, a treaty on the protection of civilians against cyberattacks, including cyberterrorism and cyberwarfare, could usefully consider and address the following issues:

- Clarification that at least certain cyberattacks are an act of violence (as that term is understood in IHL);
- Confirmation that cyberattacks may trigger an armed conflict as well as form part of the conduct of hostilities;
- A prohibition on cyberattacks directed against civilians or civilian objects, on indiscriminate cyberattacks, and on cyberattacks whose primary purpose is to terrorise civilians;
- Verification on whether states can resort to kinetic force in response to a cyberattack under *jus ad bellum*; and
- The duty to provide reparation for unlawful cyberattacks.[82]

To be valuable, a new treaty would certainly need to apply in all armed conflicts. In so doing, it could also usefully seek to resolve other longstanding issues in IHL, such as the threshold of violence needed for the existence of both international and non-international armed conflict. As the ICRC observed in its 2016 commentary on 1949 Geneva Convention I:

78 UNGA (n 19)
79 ICRC (n 6) 4.
80 ibid.
81 ibid.
82 See, eg Emanuela-Chiara Gillard, 'Reparation for Violations of International Humanitarian Law' (2003) 85(851) Intl Rev Red Cross 529–553.

> It is generally accepted that cyber operations having similar effects to classic kinetic operations would amount to an international armed conflict … However, cyber operations do not always and necessarily have such effects. Without physically destroying or damaging military or civilian infrastructure, cyberattacks might also disrupt their operation. Could these still be considered as a resort to armed force under Article 2(1) [of 1949 Geneva Convention I]? Would the low intensity approach still be appropriate for hostile actions carried out only through cyber operations? Would the threshold of harm tolerated by States affected by cyber operations be different depending on the military or civilian nature of the 'targeted' object? For the time being, these questions are left open and the law is uncertain on the subject.[83]

At the end of 2019, a General Assembly resolution offered an opportunity to begin to consider, if not necessarily resolve, some of the outstanding questions. Resolution 74/247 on countering the use of information and communications technologies for criminal purposes[84] calls for the negotiation in 2021 of a Convention on cybercrime by an open-ended intergovernmental committee of experts working within the auspices of the United Nations. While the merits of such a treaty are strongly disputed on the grounds that it is a political process preceding advice from cybercrime experts,[85] action to tackle cyberterrorism, including in a situation of armed conflict, could readily form part of the substantive provisions of the putative Convention. At the least, cyberterrorism may secure an airing within the United Nations to begin to address the Secretary-General's concerns. The 'new frontier' may result in new international law.

---

83 ICRC (n 2) paras 255 and 256.

84 UNGA Res 74/247 (27 December 2019) UN Doc A/RES/74/247. The Resolution was adopted by 79 votes to 60 with 33 abstentions.

85 See, eg, UN, 'General Assembly Approves $3.07 Billion Programme Budget as it Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-Fourth Session' (27 December 2019) UN Doc GA/12235 <https://bit.ly/2MPmyD3> accessed 17 June 2020; and Edith Lederer, 'UN Gives Green Light to Draft Treaty to Combat Cybercrime' *Associated Press News* (28 December 2019) <https://bit.ly/3hGN9zL> accessed 17 June 2020.

References

Albright D, Brannan P, and Walrond C, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment' (*Institute for Science and International Security*, 22 December 2010) <https://bit.ly/2RAyk7c> accessed 16 June 2020 <https://doi.org/10.1016/S1353-4858(10)70121-5>

Brownlie I, *International Law and the Use of Force by States* (OUP 1963) <https://doi.org/10.1093/acprof:oso/9780198251583.001.0001>

Byers M, 'The Intervention in Afghanistan—2001' in Ruys T, Corten O and Hofer A (eds), *The Use of Force in International Law: A Case-Based Approach* (OUP 2018).

Casey-Maslen S and Haines S, *Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict* (Hart 2018).

Casey-Maslen S, *Jus ad Bellum: The Law on Inter-state Use of Force* (Hart 2020).

Cyber Security Intelligence, 'Israel Responds to a Cyber Attack with Bombs' (*Cyber Security Intelligence* 10 May 2019) <https://bit.ly/39DSzrj> accessed 14 June 2020.

DePetris D,'The War in Afghanistan Turns 19 Years Old' (*Washington Examiner,* 10 July 2020*)* <https://bit.ly/3nHyjv7> accessed 20 August 2020.

Dinstein Y, *The Conduct of Hostilities Under the Law of International Armed Conflict* (3rd edn, Cambridge University Press 2016) <https://doi.org/10.1017/CBO9781316389591>

Ferguson C and Settle F, 'The Future of Nuclear Power in the United States' (*Federation of American Scientists*, 2012) <https://bit.ly/2PxlBQ7> accessed 16 June 2020.

Fidler DP, 'Cyberattacks and International Human Rights Law' in Casey-Maslen S (ed), *Weapons under International Human Rights Law* (Cambridge University Press 2014).

Findlay S and White E, 'India Confirms Cyber Attack on Nuclear Power Plant' *Financial Times* (Seoul, 31 October 2019) <https://on.ft.com/37sfPa9> accessed 17 June 2020.

Gillard EC, 'Reparation for Violations of International Humanitarian Law' (2003) 85 (851) International Review of the Red Cross <https://doi.org/10.1017/S1560775500183798>

Hammond JR, 'Newly Disclosed Documents Shed More Light on Early Taliban Offers, Pakistan Role' (*Foreign Policy Journal,* 20 September 2010*)* <https://bit.ly/2YaDt5v> accessed 13 June 2020.

Holtom P, 'United Nations Arms Embargoes Their Impact on Arms Flows and Target Behaviour: Case Study: The Taliban, 2000–2006' (2007) <https://bit.ly/2IWuOlH> accessed 12 November 2020.

International Committee of the Red Cross, 'Commentary on Article 2, 1949 Geneva Convention I' (*ICRC* 2016) <https://bit.ly/36oJa4G> accessed 10 June 2020.

International Committee of the Red Cross, 'Customary IHL Study, Rule 2. "Violence Aimed at Spreading Terror among the Civilian Population' <https://bit.ly/2ONFTT7> accessed 10 June 2020.

International Committee of the Red Cross, 'Customary IHL Study, Rule 8. Definition of Military Objectives' <https://bit.ly/2X2mHqu> accessed 11 June 2020.

International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations During Armed Conflicts* (2019) ICRC Position Paper <https://bit.ly/2TZSYim> accessed 10 June 2020.

International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions' (22 November 2019) Document 33IC/19/9.7.

International Committee of the Red Cross, 'What Does IHL Say About Terrorism' (*ICRC*, 22 January 2015) <https://bit.ly/2PxbWsY> accessed 10 June 2020.

Jahn G, 'Stuxnet Virus Penetrates Nuclear Plant, May Cause Chernobyl-Like Disaster' *The Christian Science Monitor, Associated Press* (Vienna, 31 January 2011) <https://bit.ly/2sWbcFZ> accessed 16 June 2020.

Klare MT, 'Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation' (*Arms Control Today* November 2019) <https://bit.ly/2USw1gk> accessed 16 June 2020.

Kliem T, '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' (2017) 4(2) Journal on the Use of Force and International Law <https://doi.org/10.1080/20531702.2017.1338388>

Langner R, 'Cracking Stuxnet, a 21st-Century Cyber Weapon' (*TED*, 29 March 2011) <https://bit.ly/349ErC2> accessed 16 June 2020.

Lederer EM, 'UN Gives Green Light to Draft Treaty to Combat Cybercrime' *Associated Press News* (28 December 2019) <https://bit.ly/3hGN9zL> accessed 17 June 2020.

Lyngaas S, 'Hacking Nuclear Systems is the Ultimate Cyber Threat. Are We Prepared? Nightmare Scenario' (*The Verge*, 23 January 2018) <https://bit.ly/34bW2JC> accessed 17 June 2020.

Melzer N, 'Cyberwarfare and International Law' (*United Nations Institute for Disarmament Research* 2011) 18 <https://bit.ly/2STRiqg> accessed 14 June 2020.

Rundle AA, 'International Acceptance of Kinetic Operations in Response to a Cyber Attack' (Master's Thesis, Marine Corps University 2011).

Sandoz Y, Swinarski C and Zimmermann, B (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross/Martinus Nijhoff 1987).

Saul B, 'Terrorism, Counter-terrorism, and International Humanitarian Law' in Saul B and Akande D (eds), *The Oxford Guide to International Humanitarian Law* (OUP 2020) <https://doi.org/10.4337/9781788972222.00022>

Schmitt MN, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37(3) Columbia Journal of Transnational Law <https://doi.org/10.21236/ADA471993>

Schmitt MN, 'International Humanitarian Law and the Conduct of Hostilities', in Saul B and Akande D(eds), *The Oxford Guide to International Humanitarian Law*, (OUP 2020)

Schmitt MN (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) <https://doi.org/10.1017/CBO9781139169288>

Schmitt MN, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) <https://doi.org/10.1017/9781316822524>

Schmitt MN, 'The Use of Cyber Force and International Law' in M Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (OUP 2015) <https://doi.org/10.1093/law/9780199673049.003.0053>

Smith B, 'The Need for a Digital Geneva Convention' (Transcript of Keynote Address at the RSA Conference, San Francisco, February 2017).

Smith B, 'We Need to Modernize International Agreements to Create a Safer Digital World' (*Microsoft,* 10 November 2017) <https://bit.ly/36kHjNZ> accessed 10 June 2020.

Stark H, 'Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War' (*Der Spiegel,* 8 August 2011) <https://bit.ly/2uxypPO> accessed 16 June 2020.

Turns D, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17(2) Journal of Conflict and Security Law <https://doi.org/10.1093/jcsl/krs021>

UN, 'General Assembly Approves $3.07 Billion Programme Budget as it Adopts 22 Resolutions, 1 Decision to Conclude Main Part of Seventy-fourth Session' (27 December 2019) UN Doc GA/12235 <https://bit.ly/2MPmyD3> accessed 17 June 2020.

US Senate 'Report of the Committee on Foreign Relations on the North Atlantic Treaty' (6 June 1949) Executive Report No. 8.

Wright L, *The Looming Tower: Al-Qaeda and the Road to 9/11* (Alfred P. Knopf 2006).

Cases

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), (Judgment) (Merits), (1986) ICJ Rep 14.

Prosecutor v Charles Ghankay Taylor (Judgment) SCSL-03-01-A (26 September 2013).

Prosecutor v Galić (Judgment) IT-98-29-T (5 December 2003).

Prosecutor v Galić (Judgment) IT-98-29-A (30 November 2006).

International Instruments

Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI.

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950).

Draft Comprehensive Convention on International Terrorism, in Appendix I to UN Doc A/59/894 of 12 August 2005.

International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001)

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978).

United Nations Documents

UN General Assembly Resolution 3314 (XXIX) (14 December 1974) UN Doc A/RES/3314.

UN General Assembly, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174.

UN, ‘Secretary-General Calls Cyberterrorism Using Social Media, Dark Web, ‘New Frontier’ in Security Council Ministerial Debate’ (25 September 2019) UN Doc SG/SM/19768-SC/13964.

UN Security Council Resolution 1373 (28 September 2001) UN Doc S/RES/1373.

UN General Assembly Resolution 74/247 (27 December 2019) UN Doc A/RES/74/247.