*Joanna Jarose**

RECONSIDERING THE DEFINITION OF 'ATTACK' AND 'DAMAGE' IN CYBER OPERATIONS DURING ARMED CONFLICT: EMERGING SUBSEQUENT STATE PRACTICE

Abstract

Since the 1977 *Additional Protocols* were concluded, the way the human population lives has drastically changed; technologies which had then barely been imagined have now become ubiquitous parts of our existence. The plain wording of *Additional Protocol I* guards civilians and civilian objects against 'acts of violence', physical damage and injury: the *Tallinn Manual on the International Law Applicable to Cyber Operations*, constrained by this orthodox law, has concluded that a cyber 'attack' is not really an 'attack' within the parameters of international humanitarian law ('IHL') unless it has a physical effect. This limited protection seems inadequate to guard such crucial, yet intangible, civilian infrastructure as internet connectivity and data reserves.

In the past few years, State interpretations have begun to stretch the understanding of what 'attack' and 'damage' are in the context of cyber operations. This article examines how State practice can effect change in the meaning of treaty obligations, and how a modified understanding of protections under IHL, adapted to modern priorities, can more effectively protect civilians from the effects of armed conflict. It will conclude that available State practice in the area suggests that such protections will be found, one way or another, in the existing international law framework.

* BA (Hons), MA (Res), LLB (Hons) Candidate (Adel); Research Assistant, Research Unit on Military Law and Ethics; Student Editor, *Adelaide Law Review* (2023). I would like to acknowledge the very valuable input from the anonymous reviewers, whose contributions helped significantly improve the article.

I Introduction

Cyber warfare poses a challenge for the application of international humanitarian law ('IHL'). A framework based around loss of life, physical injury and physical damage[1] is difficult to apply, mutatis mutandis, to a domain where offensive action can be undertaken without leaving any physical mark. Yet in the modern world, with everyday life so reliant on computer systems and internet connectivity, there is no disputing that a cyber operation can easily be more devastating to a civilian population than a traditional kinetic attack. Despite the potential difficulty in translation, there is a real need to set clear boundaries on belligerent actions in cyberspace.

Since 2019, many States have finally added their voices to the cyber warfare conversation. If States can reach a common agreement, they are uniquely positioned to determine the way treaty provisions are understood.[2] The majority of viewpoints that are emerging may eventually lead to a reinterpretation of 'attack' and 'damage' under existing IHL instruments such as *Additional Protocol I*.[3]

II Cyber 'Attack'?

In 2016 the United States ('US') Cyber Command led a group of coalition cyber forces (known as Joint Task Force Ares) in a cyber operation against the Islamic State's 'virtual caliphate', referred to as Operation Glowing Symphony.[4] Although the documents eventually released are heavily redacted, the purpose was ostensibly to dismantle the Islamic State propaganda unit's media stores as far as possible and to support coalition ground operations in Iraq by disabling communications

1 See, eg, *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) arts 51, 57, 85 ('*Additional Protocol I*').

2 *Vienna Convention on the Law of Treaties,* opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980) art 31(3)(b) ('*VCLT*'); International Law Commission, 'Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties' in *Report of the International Law Commission on the Work of its Seventieth Session*, UN Doc A/73/10 (2018) 11, 14 (Conclusions 7 and 8) ('ILC Draft Conclusions').

3 See *Additional Protocol I* (n 1).

4 A redacted copy was released by the National Security Archive on 21 January 2020: United States Cyber Command, *USCYBERCOM 120-Day Assessment of Operation Glowing Symphony: Executive Summary* (USCYBERCOM Document, 15 June 2016) <https://nsarchive.gwu.edu/sites/default/files/documents/6655597/National-Security-Archive-6-USCYBERCOM.pdf> ('*120-Day Assessment of Operation Glowing Symphony*'). See also Ewan Lawson and Kubo Mačák, *Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts* (Report, International Committee of the Red Cross Expert Meeting, 21–22 January 2020) 48.

and conducting other interference.[5] To date, this is the sole instance of a State-acknowledged offensive cyber campaign conducted as part of an armed conflict.[6]

Media sources, when the classified operation became public knowledge, readily referred to it as a cyber 'attack': the *New York Times* headline proclaimed that 'US Cyberattacks Target ISIS',[7] while the US Deputy Secretary of Defense was quoted as saying '[w]e are dropping cyberbombs'.[8] Other news sources reported that the participants worked to 'attack multiple targets simultaneously',[9] that the operations were followed up with 'further cyber-attacks',[10] and that US Cyber Command spent several months 'preparing for attack'.[11]

However, sources within the actual agencies involved have been more circumspect, even euphemistic. This was 'offensive cyber', according to then-Director-General of the Australian Signals Directorate, Mike Burgess.[12] It was an attempt to 'contest the enemy in the information domain', per the USCYBERCOM briefing documents.[13] So was this indeed a cyber 'attack'? Or was this something else, something lesser? Burgess was emphatic that 'all our operations are conducted in accordance with international and Australian law'.[14] But if this operation — which disabled and suppressed enemy systems in the context of armed conflict — was not an attack, then what was it, and how does international law act to constrain it?

5 *120-Day Assessment of Operation Glowing Symphony* (n 4); Lawson and Mačák (n 4); Mike Burgess, 'Director-General ASD Speech to the Lowy Institute', (Speech, Lowy Institute, 27 March 2019) <https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-speech-lowy-institute>; Jeremy Fleming, 'Director's Speech at Cyber UK 2018' (Speech, CyberUK, 12 April 2018) <https://www.gchq.gov.uk/speech/director-cyber-uk-speech-2018>.

6 Lawson and Mačák (n 4) 47.

7 David E Sanger, 'US Cyberattacks Target ISIS in a New Line of Combat', *The New York Times* (online, 24 April 2016) <https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html>.

8 Ibid.

9 Stephanie Borys, 'Licence to Hack: Using a Keyboard to Fight Islamic State', *ABC News* (online, 18 December 2019) <https://www.abc.net.au/news/2019-12-18/inside-the-islamic-state-hack-that-crippled-the-terror-group/11792958?nw=0&r=HtmlFragment>.

10 Ibid.

11 Dina Temple-Raston, 'How the US Hacked ISIS', *National Public Radio* (online, 26 September 2019) <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.

12 Burgess (n 5).

13 *120-Day Assessment of Operation Glowing Symphony* (n 4) 2.

14 Burgess (n 5).

III Applicability of IHL Principles to Cyber Warfare

The North Atlantic Treaty Organization ('NATO') recognised cyberspace as a new operational domain in 2016,[15] the same year Operation Glowing Symphony was launched. However, damaging cyber operations had been common knowledge for years prior — Estonia in 2007, Georgia in 2008 and the Stuxnet worm attack on Iranian industrial sites in 2010.[16] NATO's acknowledgement of the cyber domain came three years after the 2013 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, the first in-depth attempt to delineate the application of international law principles, including those of IHL, to conduct in cyberspace.[17] Between 2019 and 2021, many States have added their voices to the debate, confirming their views that the existing rules of IHL also apply to cyber operations.[18] Many of these perspectives were put forward as part of the United Nations ('UN') Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security ('GGE'), which is also the forum where the debate was finally put beyond doubt. The consensus report issued by the GGE,

15 North Atlantic Council, 'Warsaw Summit Communiqué' (Press Release, 9 July 2016) <https://www.nato.int/cps/en/natohq/official_texts_133169.htm>.

16 See generally: Peter Beaumont, 'Stuxnet Worm Heralds New Era of Global Cyberwar', *The Guardian* (online, 1 October 2010) <https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar>; Andrzej Kozłowski, 'Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan' (2014) 3 (Spec Ed) *European Scientific Journal* 237; Gary D Brown, 'Why Iran Didn't Admit Stuxnet was an Attack' [2011] (63) *Joint Force Quarterly* 70.

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

18 See, eg: *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266*, UN Doc A/76/136 (13 July 2021) ('*GGE Compendium 2021*'), the submissions of Australia at 6, Brazil at 17, 22, Estonia at 23, 26, Germany at 31, 36, Japan at 49, The Netherlands at 59, Norway at 66, 74, Romania at 77, Switzerland at 93, United Kingdom at 118 and the US at 138; Ministère des Armeés, *International Law Applied to Operations in Cyberspace* (Position Paper, 2019) 12 ('French Position Paper'); Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97(1) *International Law Studies* 395, 399; Ministry for Foreign Affairs, *International Law and Cyberspace: Finland's National Positions* (Position Paper, 2020) ('Finnish Position Paper'), discussed in Ministry for Foreign Affairs, 'Finland Published its Positions on Public International Law in Cyberspace', *Finnish Government* (Web Page, 15 October 2020) <https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace>.

and endorsed by the UN General Assembly, confirmed that IHL principles must be considered to apply to the cyberspace context during armed conflict.[19]

It is therefore evident that war can and will be waged online, and that this will be subject to the comprehensive set of binding international laws governing the conduct of armed conflict, including the *Geneva Conventions* and their *Additional Protocols*.[20] Even though *Additional Protocol I* has not been universally ratified, unlike the four 1949 *Geneva Conventions*, its central targeting principles are applied by non-party States as customary international law[21] (and the International Law Commission has determined they are possibly even *jus cogens*).[22] The problem is therefore not a lack of agreed law, but rather a difficulty of translation to the cyber context.

---

19 *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc A/76/135 (14 July 2021) 18 ('*GGE Final Report 2021*'). See also: Michael Schmitt, 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security* (online, 10 June 2021) <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-internationallaw-in-cyberspace/>; Adina Ponta, 'Responsible State Behavior in Cyberspace: Two New Reports from Parallel UN Processes' (2021) 25(14) *American Society of International Law: Insights* 1; Anna Maria Osula, 'In Search of a Coherent International Approach to Governing Technologies', *Observer Research Foundation: Digital Frontiers* (online, 17 October 2021) <https://www.orfonline.org/expert-speak/international-approach-to-governing-technologies/>.

20 *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, opened for signature 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950); *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, opened for signature 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950); *Geneva Convention Relative to the Treatment of Prisoners of War*, opened for signature 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950); *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, opened for signature 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950); *Additional Protocol I* (n 1); *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II)*, opened for signature 8 June 1977, 1125 UNTS 609 (entered into force 7 December 1978).

21 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law* (Cambridge University Press, 2005) vol 1, 51–2; Israeli Defence Force, *The 2014 Gaza Conflict 7 July–26 August 2014: Factual and Legal Aspects* (Report, 2015) 138; Bundesministerium der Verteidigung, *Law of Armed Conflict Manual* (Joint Service Regulation (ZDv) 15/2, 2013) 22 [136]; Norwegian Defence University College, *Manual of the Law of Armed Conflict* (Joint Service Publication, 2013) 14; Department of the Navy, *The Commander's Handbook on the Law of Naval Operations: NWP 1-14M* (Navy Warfare Library, rev ed, 2022) 5-3–5-4, 8-18 [8.10.1].

22 *Report of the International Law Commission: Seventy-First Session (29 April–7 June and 8 July–9 August 2019)* UN Doc A/74/10 (20 August 2019) 207, where the Commission discussed *jus cogens*.

Several tenets of IHL are challenged by cyber operations, primarily due to their intangible mode of action. Perhaps the most jarring disconnect is the traditional understanding that an 'attack' must involve some form of physical violence, some type of kinetic effect, such as tangible damage, injury or death. The International Criminal Court considered the definition of attack under IHL in some depth in the *Prosecutor v Ntaganda* appeal,[23] but declined to accept that it could extend beyond acts causing or intended to cause physical injury or destruction.[24] In cyber operations, where devastating consequences may be incurred without any visible physical impact, what does an 'attack' look like? What can be considered 'damage'?

IV 'Attack' and 'Damage' in *Additional Protocol I*

Part IV of *Additional Protocol I* covers protections for the civilian population in armed conflict. Article 49(1) of *Additional Protocol I* provides that '"[a]ttacks" means acts of violence against the adversary, whether in offence or defence'.[25] The term 'attack' is also used in the treaty outside pt IV,[26] but is not further defined. Whether a cyber operation is considered an 'attack' for the purposes of pt IV is important, because the majority of the rules providing specific protections to civilians and civilian objects only apply to 'attacks': art 51(2) mandates that civilians 'shall not be the object of attack'; art 51(4) prohibits '[i]ndiscriminate attacks' (which includes, under art 51(5)(b), an attack expected to be disproportionate); under art 52(1) '[c]ivilian objects shall not be the object of attack or of reprisals'; art 57 requires precautions '[w]ith respect to attacks' to minimise civilian harm, cancellation of 'attacks' expected to cause excessive harm and, under art 57(2)(c), advance warning to civilians of 'attacks' which may affect them.

Part IV also prescribes a specific metric to determine whether: (1) an attack has been subject to appropriate precautions; or (2) should be considered indiscriminate. This is based on considering likely 'loss of civilian life, injury to civilians and damage to civilian objects'.[27] Damage of this kind is therefore one of the triggers for when an attack should be considered unlawful under IHL. For example, expected 'damage to civilian objects … excessive in relation to the concrete and direct military advantage anticipated' can make an attack indiscriminate under art 51(5)(b); arts 57(2)(a)(iii) and 57(2)(b) require an attack expected to cause such disproportionate 'damage to civilian objects' to be cancelled; precautions under art 57(2)(a) must also be taken to reduce or avoid 'damage to civilian objects'. The meaning of 'damage to civilian objects' is thus of particular relevance to determine whether the requirements of

23 *Prosecutor v Ntaganda (Judgment)* (International Criminal Court, Appeals Chamber, Case No ICC-01/04-02/06 A A2, 30 March 2021). The context in which 'attack' was contemplated was whether pillage of medical equipment (a protected object) could be considered an attack: at 505–7 [1147]–[1152].

24 Ibid 511–14 [1164]–[1169].

25 *Additional Protocol I* (n 1) art 49(1).

26 See, eg, ibid arts 12, 39, 41, 42, 44, 85.

27 Ibid art 57(2).

pt IV have been or will be complied with. The 'damage' aspect is especially key in the context of a cyber attack, which may have a more subtle impact than a traditional kinetic attack and thus be unlikely to result in actual physical harm to individuals.

Whether or not cyber 'attacks' — in cases where they do not cause an impact recognisably similar to that of a kinetic attack — are constrained by these critical provisions of *Additional Protocol I* will therefore depend to a large extent on construing the meaning of 'attack' and 'damage'.

A *Diplomatic Conference and* Travaux Préparatoires

The definition of 'attacks' given in *Additional Protocol I* is brief and not overly illuminating in a cyber context: clearly in 1977 the scale of future military operations conducted by cyber means could hardly have been envisaged and the conduct of armed conflict was necessarily considered in terms of traditional ordnance.

The drafting of pt IV was largely the responsibility of Committee III of the Diplomatic Conference. Committee III had been assigned, among others, the articles covering '[g]eneral protection against effects of hostilities' and '[m]ethods and means of combat'.[28] Striking the right balance with these articles required them to 'reconcile military necessity with humanitarian aims'.[29] Therefore the definition of what, exactly, should be considered an 'attack' was of central importance to their deliberations. Interestingly, Committee III did not seem entirely satisfied with the finalised definition: the representative for the Netherlands noted that 'the Drafting Committee could possibly find a better wording'.[30] The 1987 commentary on *Additional Protocol I* indicated that the original definition intended by the drafters for 'attack' was 'to set upon with hostile action',[31] which does not necessarily mandate a resulting or intended kinetic effect. However, the reference to 'violence' was eventually retained. Committee III appeared concerned to ensure 'attacks' were not confused with 'military operations' generally, which they equated with 'movements or manoeuvres of armed forces in action'.[32]

---

28 See 'Committee III Report: CDDH/236/Rev1' in *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Application in Armed Conflicts: Geneva (1974–1977)* (Federal Political Department, 1976) vol XV, 377.

29 *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Application in Armed Conflicts: Geneva (1974–1977)* (Federal Political Department, 1978) vol VII, 286 [36].

30 *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Application in Armed Conflicts: Geneva (1974–1977)* (Federal Political Department, 1978) vol XIV, 128 [8], 85 [4] ('*Diplomatic Conference Records Vol XIV*').

31 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (International Committee of the Red Cross, 1987) 603 [1879].

32 *Diplomatic Conference Records Vol XIV* (n 30) 44 [4].

'Violence', used as the underpinning for the *Additional Protocol I* definition of 'attack', is generally associated with physical conflict — 'rough or injurious action or treatment'.[33] However, it is not necessarily so clear cut, and modern understandings of the concept may extend it to 'any unjust or unwarranted exertion of force or power'.[34] This could conceivably include acts beyond physical aggression, such as those intended to intimidate or coerce an actor into compliance. This alone broadens the possible interpretations of 'attack' pursuant to *Additional Protocol I* beyond those that involve physical impact. At the same time, this remains consistent with the distinction drawn in Committee III between, effectively, actions directed against an enemy and other non-combative actions conducted between such engagements.

It is also clear that the Committees involved in the drafting of *Additional Protocol I* did intend to cover the development of any new technologies that could be used in armed conflict.[35] It seems relevant that, in circumstances where the interpretation of a term in its application to a new context is ambiguous or unclear, the overarching intention evidenced through the *travaux préparatoires* should be taken into account to inform the meaning.[36] There is also the possibility of recourse to the *travaux* where an interpretive result is 'manifestly absurd or unreasonable'[37] — which appears applicable to any conclusion that belligerents can conduct unfettered offensive cyber operations against civilians in the context of armed conflict.

B Tallinn Manual

Michael Schmitt, general editor of the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (now in its second edition)[38] ('*Tallinn Manual 2.0*') reasoned in 2012 that *Additional Protocol I*'s 'concern was not so much with acts which were violent, but rather with those that have harmful consequences (or risk them)'.[39] 'Harm' is a very general concept not limited to physical impact[40] and at this point in Schmitt's analysis, the line of reasoning could cover even cyber attacks

---

33 *Macquarie Dictionary* (online at 10 May 2022) 'violence' (def 2).

34 Ibid (def 3).

35 See, eg: *Diplomatic Conference Records Vol XIV* (n 30) 157 [32], 234 [4]; *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Application in Armed Conflicts: Geneva (1974–1977)* (Federal Political Department, 1978) vol V, 8 [4], 126 [46], 144 [16].

36 *VCLT* (n 2) art 32(a).

37 Ibid art 32(b).

38 Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2nd ed, 2017) ('*Tallinn Manual 2.0*').

39 Michael N Schmitt, '"Attack" as a Term of Art in International Law: The Cyber Operations Context' in C Czosseck, R Ottis and K Ziolkowski (eds), *4th International Conference on Cyber Conflict* (NATO CCD COE, 2012) 283, 290 ('"Attack" as a Term of Art in International Law').

40 *Macquarie Dictionary* (online at 10 May 2022) 'harm' (def 2); *Oxford English Dictionary* (online at 10 May 2022) 'harm' (defs 1a, 1b, 2).

with no visible physical impact: such attacks may have consequences extending to dire harm to both individuals and objects.

However, Schmitt ultimately concludes that under IHL 'damage' must be physical, akin to that inflicted by traditional kinetic weapons, and that a cyber operation is not an 'attack' unless its consequences extend this far (at the very least requiring a targeted computer system or connected infrastructure to be physically repaired to function again).[41]

This is reflected as the majority view in the *Tallinn Manual 2.0*: to qualify as an attack for the purposes of IHL, a cyber operation must cause physical damage 'requir[ing] replacement of physical components'.[42]

To some extent, this seems a factually incorrect distinction, conflating physical damage with visible damage. An object can be physically damaged without appearing obviously so. Early swipe credit cards were not visually changed if they passed too close to a magnet — and yet, they were *physically* changed and rendered broken as the magnetic points recorded in the card's strip were irreversibly removed. This is a physical change involving physical damage, even if the change is not visible. So, too, is the outcome of a cyber operation which remotely forces a computer system with a traditional hard drive to remove the magnetic reference points that represent data from the disk. The disk may be reprogrammed, but the existing drive contents are physically destroyed. However, in line with the majority of *Tallinn Manual 2.0* experts, the hypothetical hard drive itself (or some physical infrastructure to which it is networked) must be broken in some way 'requir[ing] the replacement of physical components'[43] for this to be considered an attack under *Additional Protocol I*.

C *A Concerning Conclusion*

Regardless of its technological accuracy, this limiting of 'attack' and 'damage' to the physical seems interpretively questionable considering the whole point of *Additional Protocol I*: 'to reaffirm and develop the provisions protecting the victims of armed conflicts and to supplement measures intended to reinforce their application'.[44] As noted by the International Committee of the Red Cross ('ICRC') in 2019, '[s]uch an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the IHL rules on the conduct of hostilities' generally.[45] Kubo Mačák neatly underlined the resulting logical fallacy in 2015: 'many targets whose physical equivalents are firmly protected by IHL from enemy

41 Schmitt, '"Attack" as a Term of Art in International Law' (n 39) 291.

42 *Tallinn Manual 2.0* (n 38) 417 [10].

43 Ibid.

44 *Additional Protocol I* (n 1) Preamble.

45 International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* (Position Paper, November 2019) 8.

combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace'.[46]

If an attack must cause visible physical damage, shooting out the tyres of a single civilian delivery truck would be an unlawful attack, but digitally erasing the shipping manifest documentation for a national shipping company would not — despite the vastly greater potential civilian impact. It was reported in 2011 that Estonia's estimate of the financial loss caused by the 2007 cyber attacks against it was between $27.5 and $40 million[47] — despite being unsophisticated denial of service attacks which left the systems ultimately intact.[48] The attacks cut off civilian access to personal finances, media and communication.[49] And yet, under the *Tallinn Manual 2.0* majority view none of these actions (if carried out in the context of an armed conflict) could be characterised as an attack subject to IHL targeting restrictions — and would therefore be acceptable to employ against civilians. In this view, Operation Glowing Symphony was not an 'attack' based on a single word ('violence') in *Additional Protocol I* — and as a result, it theoretically required no distinction or proportionality assessment and no consideration of precautions in means and methods.

If the target had not been a terrorist organisation, but another State, could this be accepted?

On the day Russia launched its invasion of Ukraine, a multi-pronged cyber attack was launched against Viasat's KA-SAT network, which provided much of the internet services to Ukraine including to its government. The hackers exploited an error in Viasat's VPN setup to infect the network servers with malware and wipe the flash memory from over 45,000 individual modems.[50] This had strategic military advantages for Russia, but — if classified as an attack under *Additional Protocol I* — was also clearly indiscriminate, as the malware targeted and disabled

46 Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law' (2015) 48(1) *Israel Law Review* 55, 78.

47 'EU Seeks Unified Cybersecurity Regime', *United Press International* (online, 16 June 2011) <https://www.upi.com/Top_News/Special/2011/06/16/EU-seeks-unified-cyber security-regime/87891308219420/>.

48 NATO Strategic Communications Centre of Excellence, *Hybrid Threats: A Strategic Communications Perspective* (Report, 2019) 52, 54; Steve Ranger, 'What is Cyberwar? Everything You Need to Know About the Frightening Future of Digital Conflict', *ZDNet* (online, 4 December 2018) <https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/>.

49 Damien McGuinness, 'How a Cyber Attack Transformed Estonia', *BBC News* (online, 27 April 2017) <https://www.bbc.com/news/39655415>.

50 Katrina Manson, 'The Russian Hack Everyone is Finally Talking About' (New York, 6 March 2023) *Bloomberg Businessweek* 42, 45. See also Cynthia Brumfield, 'Incident Response Lessons Learned from the Russian Attack on Viasat', *CSO* (online, 16 August 2023) <https://www.csoonline.com/article/649714/incident-response-lessons-learned-from-the-russian-attack-on-viasat.html>.

end-user devices in the system regardless of whether they were relied on by civilians or combatants. Many of these end-users were not even located in Ukraine, but rather in other neutral States across the world.[51] Although Russia denied responsibility for the hack,[52] it provides a powerful example of how impactful cyber operations can be in armed conflict — and how important it is to control their potential impact on civilian populations.

D *Beyond Visible and Physical Damage*

Rule 92 of the *Tallinn Manual 2.0* notes the view of some of its group of experts that a cyber operation may qualify as an attack even where there is no visible physical damage, either if repair requires reinstallation of the operating system or other data,[53] or if it results in any loss of functionality howsoever caused.[54] Although these are presented as minority perspectives, this seems a logical reflection of the potentially serious disruptive effect to civilian lives that may result from such operations.

In the light of the treaty's object and purpose, Schmitt's initial statement above on *Additional Protocol I*'s concern with acts 'that have harmful consequences (or risk them)'[55] seems persuasive. Perhaps a more reasonable general definition of an attack or 'acts of violence'[56] in a cyber context is an operation producing such consequences.[57] The recently updated US Department of Defense dictionary provides that a 'cyberspace attack' causes 'degradation, disruption, or destruction' of its objective.[58] Arguably this definition summarises how 'damage' in the context of cyber warfare ought to be generally conceived of. A hostile action which inflicts such 'damage' should be considered a form of 'violence' under *Additional Protocol I*, making such an action an attack subject to all the targeting requirements mandated by pt IV of that *Protocol*.

However, regardless of the protections that *Additional Protocol I* should provide, the *Tallinn Manual 2.0*'s majority interpretation is reasonable given the general absence, in 2017, of any decisive State practice or agreement with interpretive weight under arts 31(3) or 32 of the *Vienna Convention on the Law of Treaties* ('*VCLT*'). Interpretation of a treaty term can only be based on relevant available materials, and manuals (aiming for wider utility) generally take a conservative approach to the law.

---

51 Manson (n 50) 44.

52 Ibid.

53 *Tallinn Manual 2.0* (n 38) 417 [10].

54 Ibid 417–18 [11].

55 Schmitt, '"Attack" as a Term of Art in International Law' (n 39) 290.

56 *Additional Protocol I* (n 1) art 49(1).

57 Harvard University Program on Humanitarian Policy and Conflict Research, *Commentary to the HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press, 2013) 126–7 ('*HPCR Manual*').

58 United States Department of Defense, *DOD Dictionary of Military and Associated Terms* (2021) 55 ('*US DOD Dictionary*').

It is, in fact, noted in rule 92 that the Group of Experts considered how to categorise a cyber operation that 'does not cause the type of damage set forth above, but that results in large-scale adverse consequences'[59] and concluded that 'although there might be logic in characterising the operation as an attack, the law of armed conflict does not presently extend this far'.[60] Any broadly accepted interpretation of IHL concepts will always require the support of States.

V Subsequent State Practice and Interpretation Under the *Vienna Convention on the Law of Treaties*

In the context of cyber operations, State practice may influence the interpretation of terms in *Additional Protocol I* under both primary and supplementary interpretive means. Given that the terms 'attack' and 'damage' are also quite general, there is a further argument that they may have an intrinsically evolving meaning which can also be confirmed by recourse to State practice.

A *Primary Interpretation: Article 31(3)(b)*

Article 31(3)(b) of the *VCLT* provides that the very meaning of a treaty provision must be informed by 'any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation'.[61] The International Law Commission has found that this is not merely a supplementary means of interpretation or confirmation, but can expand or narrow the primary meaning derived from art 31(1).[62]

As a result, in circumstances where all States parties eventually reach some express or implied agreement between them about how a treaty should be interpreted in various contexts — for example, about what 'attack' means in *Additional Protocol I* as applied to cyber operations — this can have a practical impact on how the treaty operates. The catch is that for State practice to be applicable as a primary method of interpretation it must reflect a 'sufficient common understanding' between the parties, which such parties recognise as and intend to be evidence of the correct interpretation of the treaty:[63] this genuinely requires that *all* parties 'have taken a position regarding the interpretation'.[64] So while it is theoretically possible for States to reach such a position, the likelihood seems practically remote.

---

59 *Tallinn Manual 2.0* (n 38) 418 [13].

60 Ibid.

61 *VCLT* (n 2) art 31(3)(b).

62 International Law Commission, *Second Report on Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties by Georg Nolte, Special Rapporteur*, UN Doc A/CN.4/671 (26 March 2014) 120–1 [20].

63 Ibid 125 [43], 128 [55]; ILC Draft Conclusions (n 2) 75–7.

64 ILC Draft Conclusions (n 2) 43.

B *Supplementary Interpretation: Article 32*

However, under art 32 of the *VCLT*, even subsequent practice which does not demonstrate specific agreement on interpretation among party States may be used to help determine the meaning of treaty provisions.[65] Resort to such means is permissible if interpretation under art 31 either 'leaves the meaning ambiguous or obscure',[66] or, gives a result which is 'manifestly absurd or unreasonable'.[67] This seems relevant on both counts, given the ongoing confusion discussed above surrounding cyber 'attack' and the 'damage' caused, and the illogical results of an orthodox interpretation of these terms (which ostensibly permits various offensive action against civilians and civilian infrastructure otherwise protected by IHL).

C *Evolving Meaning of General Terms*

The International Court of Justice has also noted that general terms used in long-standing treaties are expected to evolve in meaning over time: 'the parties must be presumed, as a general rule, to have intended those terms to have an evolving meaning'.[68] Such intention is confirmed via State practice[69] — a process we appear to be witnessing in real time with the above reframing of 'attack' and 'damage'. This natural evolution of language can even 'result in a departure from the original intent on the basis of a tacit agreement'.[70] With this consideration added to the interpretive influence of State practice, there seems little remaining basis for insisting on the retention of some static, historical meaning for these concepts when States intercede.

VI The Emergence of Subsequent State Practice

Until recently, States have seemed reluctant to publicise their views on the law governing cyber operations. This is not surprising — States must strike a balance between, on the one hand, protecting their populations from the fallout of hostile cyber operations and, on the other, retaining their own flexibility and freedom in conducting defence and intelligence activities. There is a limiting finality in any declaration that a certain type of cyber operation is either lawful or unlawful.

Since 2019, however, a number of States are finally starting to take a public stance in regard to some of the interpretive difficulties introduced by the cyber operational

65 *VCLT* (n 2) art 32; ILC Draft Conclusions (n 2) 13–14, Conclusions 2(4), 4(3), 5(1), 6(3), 7(2). See also Irina Buga, *Modification of Treaties by Subsequent Practice* (Oxford University Press, 2018) 75–6.

66 *VCLT* (n 2) art 32(a).

67 Ibid art 32(b).

68 *Dispute regarding Navigational and Related Rights (Costa Rica v Nicaragua) (Judgment)* [2009] ICJ Rep 213, 243 [66] ('*Costa Rica v Nicaragua*').

69 ILC Draft Conclusions (n 2) 14 (Conclusion 8).

70 *Costa Rica v Nicaragua* (n 68) 242 [64].

domain. The most recent UN Governmental Group of Experts, which submitted its final report in 2021,[71] prompted a wide array of submissions from States[72] which added significantly to the number now 'on the record' regarding cyber operations and IHL.

Although there is not yet consensus between all participants, States' views demonstrate an emerging convergence of perspectives. The views publicised thus far, applied under art 32 of the *VCLT* to resolve the ambiguity of how cyber 'damage' may be categorised under *Additional Protocol I*, on balance support a less restrictive interpretation of 'attack' and 'damage'.[73] It is an encouraging sign that IHL protections extended to cyber infrastructure are more significant than may have been previously understood.

This is a fast-moving area — unusually so in the realm of international law. While this article canvasses many State positions available as at the time of writing, more States are contributing their perspectives each year. Further UN initiatives will continue to prompt more State engagement with this issue, such as the submissions given in response to the ongoing Open Ended Working Group on Information and Communication Technologies.[74] As States continue to set out their understanding, a firmer or varied conclusion about the appropriate definition of 'attack' and 'damage' applicable to cyber operations may become possible. The Cyber Law Toolkit project, run jointly by six partner institutions, keeps an accessible online register of national positions as they are released which can be consulted for more information about this ongoing dialogue.[75]

A *Specific Statements About 'Attack' in the IHL Context*

Of direct relevance to the conundrum about cyber 'attack', several States have specifically noted that a cyber operation may be considered an 'attack' even where it does not result in any physical effects — and, as follows, that 'damage' therefore does not have to be physical in nature.

For example, in 2019 France's Ministère des Armeés provided that

> [c]ontrary to the *Tallinn Manual*, France considers that an attack within the meaning of Article 49 of AP I may occur even if there is no human injury or loss of life, or physical damage to goods. Thus, a cyberoperation constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were

71 *GGE Final Report 2021* (n 19).

72 *GGE Compendium 2021* (n 18).

73 Under *VCLT* (n 2) art 31(3)(a).

74 Associated State submissions available at 'Open-Ended Working Group on Information and Communication Technologies', *United Nations Office for Disarmament Affairs* (Web Page) <https://meetings.unoda.org/meeting/57871/documents>.

75 See 'Category: National Position', *Cyber Law Toolkit* (Web Page, 2021) <https://cyberlaw.ccdcoe.org/wiki/Category:National_position>.

> implemented, including temporarily or reversibly, where action by the adversary is required in order to restore the infrastructure or the system.[76]

This notably not only eschews the requirement for physical damage, but explicitly includes as potential attacks those which cause only temporary interruptions in functioning. So long as the adversary has to take some action to restore functionality as a consequence of the cyber operation, in the opinion of France this can be considered a cyber 'attack'.

One of the more recent national positions released, that of Costa Rica, adopts a similar position that even temporary loss of function can be 'damage' and the operation resulting in them can therefore be an 'attack' under IHL.[77] It provides that

> Costa Rica defines a cyber-attack under IHL as any conduct initiated in or through cyberspace that is designed or can be reasonably expected to cause injury or death to persons or damage or destruction to objects. … Costa Rica understands damage to include the disabling — temporary or permanent, reversible or not — of the targeted computer, system, or network. For the avoidance of doubt, this means that the existence of physical damage to objects or injury or death to persons is not required for an operation to constitute an attack under IHL.[78]

Costa Rica specifically indicates that 'encrypting data through ransomware, despite being temporary and reversible, would be considered an attack under IHL and therefore must not be directed against civilian systems'.[79]

Germany's submission to the UN compendium notes that it considers a cyber operation an 'attack' when it 'cause[s] harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems or on physical objects or persons'[80] and further specifies that '[t]he occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required for an attack in the sense of art 49 para 1 [of] *Additional Protocol I*'.[81] This perspective, like that of France, is a notable expansion of the traditional understanding of 'attack' — not just extending the definition to include instances where the impact is not felt in terms of physical damage, but also including a very wide array of harmful effects to both the systems themselves and to people and

---

76 French Position Paper (n 18) 13 (emphasis omitted).

77 Ministry of Foreign Affairs of Costa Rica, *Costa Rica's Position on the Application of International Law in Cyberspace* (Position Paper, 21 July 2023) 13 [49] <https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf> ('Costa Rican Position Paper').

78 Ibid.

79 Ibid.

80 *GGE Compendium 2021* (n 18) 36–7 (submission of Germany).

81 Ibid 37.

objects reliant on them. Under this framing, even some relatively innocuous cyber operations that are limited in impact to 'inconvenience, irritation, stress [or] fear'[82] could arguably be considered an 'attack'.

Ireland adopted a similar position in 2023, indicating that '[t]he concept of an "attack" in IHL … extends to cyber operations expected to cause loss of functioning to networks or electronic systems'.[83] As also argued in this article, Ireland reasons that a more restrictive interpretation of attack would leave civilians and civilian objects unprotected by IHL, which 'would not be consistent with the object and purpose of the *Geneva Conventions* and their *Additional Protocols*'.[84]

Pakistan's 2023 national position paper presents a very clear view that a cyber attack is capable of being considered an 'attack' in IHL.[85] It also sets a relatively low threshold for this application, including as examples of prohibited attack: 'employment of cyber and other digital weapons which undermines the confidentiality, integrity, and the availability of a critical civilian infrastructure';[86] '[a]ny attempt to delete, destroy and manipulate the data essential for the smooth functioning of [such infrastructure]'; and '[e]mployment of cyber and other digital technologies to spread fear and chaos among the civilian population through disinformation'.[87]

Italy's late 2021 position paper maintains that an attack must be 'an act of violence', in accordance with *Additional Protocol I*, but specifies an action could be classified as such if it results in 'disruption in the functioning of critical infrastructure' — a clear shift in the understanding of what can be considered 'damage' under IHL.[88]

The US mentions that '[*i*]*n addition* to the potential physical damage that a cyber activity may cause … parties must assess the potential effects of a cyber attack on civilian objects that are not military objectives'[89] — this view does not specify what the further 'potential effects' to be considered must be, but clearly an attack is conceptualised as having an impact beyond the physical which is relevant to

---

82 Cf *HPCR Manual* (n 57) 20, 96.

83 Ireland Department of Foreign Affairs, *Position Paper on the Application of International Law in Cyberspace* (Position Paper, July 2023) [31] ('Irish Position Paper').

84 Ibid.

85 Pakistan Mission to the United Nations, *Pakistan's Position on the Application of International Law in Cyberspace* (Position Paper, 3 March 2023) 3 [14] ('Pakistani Position Paper').

86 Pakistan defines such infrastructure very broadly, including 'but is not limited to health, transportation, energy, banking and financial sector, civilian logistical supply chains, undersea fibre optic cables, satellites, and other telecommunication networks': ibid.

87 Ibid.

88 Ministry of Foreign Affairs and International Cooperation, Presidency of Council of Ministers and the Ministry of Defence, *Italian Position Paper on 'International Law and Cyberspace'* (Position Paper, Republic of Italy, December 2021) 9–10.

89 *GGE Compendium 2021* (n 18) 138 (submission of the US) (emphasis added).

IHL requirements. As previously mentioned, the US Department of Defense *DOD Dictionary of Military and Associated Terms* also defines 'cyberspace attack' as '[a]ctions taken in cyberspace that create noticeable denial effects (ie, degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain',[90] again apparently acknowledging that even where the direct impact of an operation is confined to cyberspace this can still constitute an 'attack' if the effects are of sufficient scale.

However, this wave of State practice is not uniform. Israel's 2020 position paper accords with the *Tallinn Manual 2.0* majority position, in stating that '[o]nly when a cyber operation is expected to cause physical damage, will it satisfy this element of an attack under LOAC'.[91] Supporting this understanding is their observation that 'practices such as certain types of electronic warfare, psychological warfare, economic sanctions, seizure of property, and detention have never been considered to be attacks' due to the lack of physical damage caused, and there is 'no other specific rule to the contrary that has evolved in the cyber domain'.[92] Denmark's 2023 position paper expresses a similar view, indicating that 'a cyber operation will constitute an attack if it can be reasonably expected to cause injury, death or physical damage to individuals or objects'.[93] Denmark further indicates that data itself should not be considered an object for the purposes of IHL, and an operation to destroy such data would only be classified as an attack where 'the destruction of data foreseeably results in injury, death or physical damage'.[94]

The Inter-American Juridical Committee of the Organization of American States canvassed numerous State members about cyber operations and international law in 2019. The responses were usefully summarised in November 2020.[95] Although the full-text State views do not appear to be publicly available, the summary indicates that perspectives vary between the respondent States. Guatemala and Ecuador indicated that a cyber operation leading to loss of functionality (with or without visible damage) can be an attack under IHL,[96] while Chile and Peru took the view that to meet this threshold would specifically require damage akin to a kinetic attack.[97] However, the report does note that Peru's response is 'a bit ambiguous, as it appears to rely on *jus ad bellum* materials to identify the standards for an

90 *US DOD Dictionary* (n 58) 55.

91 Schöndorf (n 18) 400.

92 Ibid.

93 Jeppe Mejer Kjelgaard and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' (2023) *Nordic Journal of International Law* 1571–8107: 1–10, 9–10 ('Danish Position Paper').

94 Ibid 10.

95 Department of International Law of the Secretariat for Legal Affairs, *Improving Transparency: International Law and State Cyber Operations* (Report, Inter-American Juridical Committee, 1 November 2020) Annex B.

96 Ibid 45–6 [32].

97 Ibid 45 [31].

IHL attack'.[98] Bolivia and Guyana also responded to the inquiry, but were 'more equivocal' on this specific issue.[99]

Other States which have not attempted to conclusively expand or limit the definition of 'attack' or 'damage' have nevertheless raised a need for further clarification of how IHL applies to cyber operations. These include Estonia,[100] Kenya,[101] and Switzerland.[102]

VII Other Noted Protections Against Cyber Attacks Under IHL

Some States have also raised other mechanisms within IHL which provide protections to civilian populations from cyber warfare, even if the definition of an 'attack' cannot be expanded beyond operations with physical consequences akin to those of a kinetic attack.

A *General Civilian Protections and Basic Rule*

Australia, for example, notes the 'general protections afforded to the civilian population … against dangers arising from military operations'[103] which belligerents must take into account in all their actions potentially having an adverse impact. This requirement is also emphasised by Pakistan and by Israel (despite the latter State not currently of the view that the concept of 'attack' should be interpreted broadly in cyber operations).[104] Germany draws attention to the obligation to 'take constant care to spare the civilian population',[105] as does Finland in its 2020 position paper.[106] Brazil quotes the Martens clause as authority that civilian protections must still apply in cases 'where IHL is silent or ambiguous'.[107]

Of relevance to these perspectives, it should be noted that the basic rule of *Additional Protocol I*, art 48, does not actually proscribe 'attacks' against civilians per se. Instead, it forbids parties to the conflict from directing their 'operations' against civilians or civilian objects. Although the 1987 commentary suggests that this relates to 'military operations during which violence is used', it simultaneously

98 Ibid 45 n 76.

99 Ibid 46 [33].

100 Ibid 27 (submission of Estonia).

101 Ibid 54 (submission of Kenya).

102 *GGE Compendium 2021* (n 18) 94 (submission of Switzerland).

103 Ibid 6 (submission of Australia).

104 Pakistani Position Paper (n 85) 3–4; Schöndorf (n 18) 401.

105 *GGE Compendium 2021* (n 18) 38 (submission of Germany).

106 Finnish Position Paper 2020 (n 18) 7.

107 *GGE Compendium 2021* (n 18) 23 (submission of Brazil), citing *Additional Protocol I* (n 1) art 1.

provides that this 'refers to all movements and acts related to hostilities that are undertaken by armed forces',[108] the latter of which is more closely supported by the Diplomatic Conference records.[109] Given the extensive use of the term 'attack' throughout *Additional Protocol I*, the intentional use of the term 'operations' in art 48 (and, similarly, art 51(1)) must have some significance; the two cannot be considered interchangeable, and 'operation' must encompass some military activities beyond 'attacks'. It therefore seems strongly arguable — and was raised by Heather Harrison Dinniss as far back as 2012 — that even if offensive cyber cannot be considered to fall within the concept of 'attack', it still can only be employed against military objectives and military personnel.[110]

B *Proportionality, With or Without 'Attack'*

Multiple States also raise — regardless of whether they explicitly support the expansion of the definition of 'attack' to include instances of non-physical damage — that due to the complexity and interconnectedness of the cyber environment and the difficulty of assessing the impact of a cyber operation, very thorough proportionality assessments are required in conducting such operations and the duty to take all feasible precautions to reduce harm to civilians is even more crucial. Switzerland, for example, notes that 'the obligation to take all precautionary measures practically possible to spare civilians and civilian objects plays a particularly important role in the use of cyber means and methods of warfare'.[111] Similar sentiments are echoed by Brazil,[112] the US,[113] Denmark[114] and France.[115] France, in particular, suggests that proportionality assessments in cyber operations must consider all direct and indirect damage that may result, such as the scale of impact of malfunctioning systems.[116]

C *Data as a Protected Civilian Object*

Several States have also expressed a belief that civilian data is in fact a civilian 'object' requiring protection[117] (as afforded to civilian objects by arts 48, 49, 51 and especially 52 of *Additional Protocol I*). This is contrary to the majority view in the *Tallinn Manual 2.0* — which suggested that general civilian data per se is

---

108 Sandoz, Swinarski and Zimmermann (n 31) 600 [1875].

109 *Diplomatic Conference Records Vol XIV* (n 30) 44 [4].

110 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012) 199.

111 *GGE Compendium 2021* (n 18) 94 (submission of Switzerland).

112 Ibid 23 (submission of Brazil).

113 Ibid 139 (submission of the US).

114 Kjelgaard and Melgaard, 'Danish Position Paper' (n 93) 10.

115 French Position Paper (n 18) 16.

116 Ibid.

117 *GGE Compendium 2021* (n 18) 37 (submission of Germany), 78 (submission of Romania); French Position Paper (n 18) 14; Costa Rican Position Paper (n 77) 13–14 [50].

only protected in cases where injury, death or other physical damage would result from its destruction.[118] If civilian data can be considered to have status as a civilian object, this would engage the protective principles of distinction, proportionality and precautions in means and methods for any entity reliant on such civilian data.

Of course, this protection may be subsidiary where States have also supported a reconceptualisation of 'attack' to include non-visible damage. As summarised in an article written by three ICRC legal advisers:

> if data are deleted or manipulated in a manner that is designed or expected to cause, directly or indirectly, death or injury to a person, or damage to (*including — in our view — by disabling*) a physical object, the operation is an attack regardless of whether data themselves constitute objects for the purpose of IHL.[119]

VIII Relevant Statements Regarding *Jus ad Bellum*

In cases where States have not specifically addressed the *jus in bello* definition of 'attack', they may nevertheless identify disruptive cyber operations as a potential 'use of force' even where they do not inflict physical damage — confirming, if nothing else, that such operations would not be passively accepted. Thresholds specified in regard to armed attack, which enlivens a right to act in self-defence,[120] may be particularly relevant. This is because at least two States which explicitly recognise that 'attack' under IHL can include loss of functioning in cyber assets have nevertheless specified that there is a higher threshold (requiring damage akin to a kinetic attack) for an *initial* attack capable of instigating an armed conflict.[121] If a State considers that even an 'armed attack' in the *jus ad bellum* context potentially does not require observable damage, this may suggest they would ascribe to a fairly low threshold for 'attack' in the context of IHL.

States which have made potentially relevant statements include:

- Australia, which indicates that in determining if a cyber activity amounts to a use of force, it is relevant whether the action is likely to result in 'damage or destruction (*including to their functioning*) to objects or critical infrastructure';[122]
- The Netherlands, specifying that 'a cyber operation with a very serious financial or economic impact may qualify as the use of force';[123]

---

118 *Tallinn Manual 2.0* (n 38) 416 [6], 437 [6].

119 Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, 'Twenty Years On: International Humanitarian Law and The Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (2020) 102(913) *International Review of the Red Cross* 287, 317 (emphasis added).

120 *Charter of the United Nations* art 51.

121 See, eg: Irish Position Paper (n 83) [30]; Costa Rican Position Paper (n 77) 12 [42].

122 *GGE Compendium 2021* (n 18) 5 (submission of Australia) (emphasis added).

123 Ibid 58 (submission of The Netherlands).

- Norway, which indicates that 'a cyber operation causing severe disruption to the functioning of the State such as the use of crypto viruses or other forms of digital sabotage … could amount to the use of force in violation of Article 2(4)';[124]
- Poland, which notes that where a cyber attack 'caus[es] similar effects to those caused by a classic armed attack' it may be considered equivalent, and gives the example of a cyber operation which damages a power plant, deactivates a missile defence system or takes control of an aircraft or ocean vessel in order to cause a collision;[125] and
- Singapore, which notes that 'malicious cyber activity may amount to an armed attack even if it does not necessarily cause death, injury, physical damage or destruction' and provides the example of 'a targeted cyber operation causing sustained and long-term outage of Singapore's critical infrastructure'.[126]

Despite the context in which these were raised, they do add to the broader reframing of the significance and potential severity of cyber operations in relation to conflict between States.

IX A Position of Compromise

An expansion of the concepts of 'attack' and 'damage' under *Additional Protocol I* to encompass all situations where there is non-trivial loss of functionality provides significantly greater protection to civilians affected by armed conflict. Modern examples have clearly demonstrated the chaos and significant loss that can result from cyber operations.[127] Requiring that military forces consider more broadly potential collateral damage beyond the physical impact of their actions is now simply mandated by the world's reliance on digital infrastructure.

A more nuanced interpretation of 'attack' and 'damage', via the operation of State practice, can only assist with upholding the object and purpose of *Additional Protocol I*. This would have flow-on effects in expanding the protective mechanisms accorded to civilians and civilian institutions — especially in application to proportionality assessments and the obligation to take precautions in the means and method of attack.[128] This would not prevent military forces from making use of disabling cyber operations, but would firmly (and appropriately) disallow civilian cyber infrastructure to be their target in armed conflict. At the same time, it would require military forces to comprehensively assess the collateral impact to civilian systems when conducting such operations against valid military targets, even where this is achieved without any damage to infrastructure hardware.[129]

---

124 Ibid 70 (submission of Norway).

125 Council of Ministers, *The Republic of Poland's Position on the Application of International Law in Cyberspace* (Position Paper, Republic of Poland, December 2022) 5 [4].

126 *GGE Compendium 2021* (n 18) 84 (submission of Singapore).

127 See, eg, Beaumont (n 16).

128 Under *Additional Protocol I* (n 1) arts 57(2)(a)(ii)–(iii), 57(2)(b).

129 Ibid art 52.

X Conclusion

At this stage, there are only limited indications of how States interpret *Additional Protocol I* as it applies to a cyber 'attack' and 'damage' under IHL. Many more States remain absent from the conversation, while others have provided only preliminary and tentative views. However, the State positions available suggest that States are not reluctant to reconsider and reinterpret IHL principles to fill the gaps identified in their application to the cyber domain.

States have put forward multiple mechanisms in extant law that protect civilians in armed conflict situations from the impact of cyber operations. The 2015 Group of Governmental Experts, comprised of 20 State contributors, had proposed as a 'voluntary, non-binding norm' that a State should 'not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public'.[130]

In 2019, the year that the subsequent GGE began its deliberations, Michael Schmitt resorted to policy recommendations intended to shore up a system of black letter law which — in his view, taking the traditional perspective of 'attack' — failed to ensure the intended protections for civilian populations.[131] The influx of State viewpoints discussed above followed soon after; these provided a stark and perhaps unexpected contrast of view. In them is an overriding confirmation that, one way or another, cyber operations which impose dire consequences on civilians will not be considered lawful, regardless of whether they cause damage in the traditional, kinetic sense. The litany of considerations States stipulate must be accounted for by those planning cyber operations is reminiscent of another minority position stated in the *Tallinn Manual 2.0*: 'should an armed conflict involving such cyber operations break out, the international community would generally regard them as an attack'.[132] There is every expectation, based on the emerging State practice, that this will hold true. As more comprehensive State practice enables a firm reinterpretation, it is likely that the crucial protections IHL provides to civilian populations affected by war will be fully transposed to the cyber context in accordance with the overriding object and purpose of this body of law.

130 Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, *Report of the Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174 (22 July 2015) 8 [13(f)]. This was confirmed by the subsequent 2019–21 GGE in *GGE Final Report 2021* (n 19) 8.

131 Michael Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations' (2019) 101(1) *International Review of the Red Cross* 333, 343.

132 *Tallinn Manual 2.0* (n 38) 418 [13].