International Review of the Red Cross, Page 1 of 48.
doi:10.1017/S1816383120000387

INTERNATIONAL REVIEW of the Red Cross

Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts

Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann*

Laurent Gisel is Head of the Arms and Conduct of Hostilities Unit in the Legal Division of the International Committee of the Red Cross (ICRC) in Geneva. Between 2013 and 2020, he was the ICRC's Senior Legal Adviser, Cyber Team Leader and file holder for the rules governing the conduct of hostilities under international humanitarian law, including their application during urban warfare, cyber operations, and outer space operations.

Dr Tilman Rodenhäuser is a Legal Adviser at the ICRC, working on cyber operations during armed conflict, non-State armed groups, and detainee transfers.

* An earlier version of this article has been published by the same authors under the title "The Applicability and Application of International Humanitarian Law to Cyber Warfare", *Chinese Review of International Law*, Vol. 32, No. 4, 2019. It has been substantially updated and broadened for publication in this issue of the *Review*. This article was written in a personal capacity and does not necessarily reflect the views of the ICRC.

Dr Knut Dörmann is Head of the ICRC's Delegation to the EU, NATO and the Kingdom of Belgium (Brussels), and former Chief Legal Officer and Head of the Legal Division (2007–19). Prior to that, he was Deputy Head of the ICRC's Legal Division (2004–07) and a Legal Adviser to the ICRC (1999–2004), including on cyber operations.

Abstract

The use of cyber operations during armed conflicts and the question of how international humanitarian law (IHL) applies to such operations have developed significantly over the past two decades. In their different roles in the Legal Division of the International Committee of the Red Cross (ICRC), the authors of this article have followed these developments closely and have engaged in governmental and non-governmental expert discussions on the subject. In this article, we analyze pertinent humanitarian, legal and policy questions. We first show that the use of cyber operations during armed conflict has become a reality of armed conflicts and is likely to be more prominent in the future. This development raises a number of concerns in today's increasingly cyber-reliant societies, in which malicious cyber operations risk causing significant disruption and harm to humans. Secondly, we present a brief overview of multilateral discussions on the legal and normative framework regulating cyber operations during armed conflicts, looking in particular at various arguments around the applicability of IHL to cyber operations during armed conflict and the relationship between IHL and the UN Charter. We emphasize that in our view, there is no question that cyber operations during armed conflicts, or cyber warfare, are regulated by IHL – just as is any weapon, means or methods of warfare used by a belligerent in a conflict, whether new or old. Thirdly, we focus the main part of this article on how IHL applies to cyber operations. Analyzing the most recent legal positions of States and experts, we revisit some of the most salient debates of the past decade, such as which cyber operations amount to an "attack" as defined in IHL and whether civilian data enjoys similar protection to "civilian objects". We also explore the IHL rules applicable to cyber operations other than attacks and the special protection regimes for certain actors and infrastructure, such as medical facilities and humanitarian organizations.

Keywords: cyber operations, armed conflict, cyber warfare, human cost, international humanitarian law.

: : : : : : :

The use of cyber operations during armed conflicts and the question of how international humanitarian law (IHL) applies to such operations have developed significantly over the past two decades. This finding is true at the operational, legal and political levels. Operationally, the use of cyber operations during armed conflict has become a reality of armed conflicts and is likely to be more prominent in the future. This development raises a number of concerns in

today's ever more cyber-reliant societies, in which malicious cyber operations risk causing significant disruption and harm to humans. At the political and legal levels, through multilateral processes States have achieved agreement on some aspects of the legal and normative framework regulating cyber operations; however, the application of IHL to cyber operations during armed conflict remains the subject of intense discussion. A few States have published positions on how IHL applies to cyber operations during armed conflicts, and a wealth of academic studies exist on the matter, yet key issues remain controversial and lack agreement among States and other experts, or require further analysis. These include the notion of "attack", the question of how civilian data are protected against harmful cyber operations, and which IHL rules apply to cyber operations other than attacks. In their different roles in the Legal Division of the International Committee of the Red Cross (ICRC), the authors of this article have followed these developments and debates closely and have engaged in governmental and non-governmental expert discussions on the applicability and application of IHL to cyber operations during armed conflicts since their beginning.

The ICRC has recently published a comprehensive institutional position on *International Humanitarian Law and Cyber Operations during Armed Conflicts*, which was submitted to the United Nations (UN) Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG).[1] In this article, we expand on this position and first explain why the potential human cost of cyber operations is a humanitarian concern. We then underline that IHL applies to – and therefore restricts – cyber operations during armed conflicts and examine different States' views on this subject. Third, we analyze when cyber operations may trigger an armed conflict and how this threshold relates to the prohibition of the use of force and the right to self-defence under the UN Charter and customary international law. In the last and most substantial part of the article, we delve into some of the long-standing questions on how IHL applies to cyber operations during armed conflicts and what positions States have taken on some of the key issues.

Operationally, the use of cyber technology has become a reality in today's armed conflicts and is likely to increase in the future. Some States have acknowledged publicly that they have conducted cyber operations in ongoing armed conflicts. In particular, the United States, the United Kingdom and Australia have disclosed that they used cyber operations in their conflict against the Islamic State group.[2] There are also public reports suggesting that Israel used

1 ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Position Paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019, available at: www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts (all internet references were accessed in August 2020). Also available in the "Reports and Documents" section of this issue of the *Review*.

2 See, in particular, Mike Burgess, Australian Signals Directorate, "Offensive Cyber and the People Who Do It", speech given to the Lowy Institute, 27 March 2019, available at: www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm; Paul M. Nakasone, "Statement of General Paul

cyber operations against Hamas – and allegations that Hamas used cyber operations against Israel.[3] Furthermore, cyber operations have affected other countries involved in armed conflicts, such as Georgia in 2008,[4] Ukraine in 2015–17[5] and Saudi Arabia in 2017,[6] though the authors of these cyber attacks remain unknown and attribution of responsibility is contested. It is therefore unclear whether these operations had a nexus to the respective armed conflicts and thus whether IHL applied. Moreover, there have been reports of cyber operations by States in other situations where the legal classification may not be straightforward, including in what is sometimes referred to as a "grey zone".[7] These examples show an increase in military cyber operations over the past decade – a change in warfare that might continue. Indeed, an increasing number of States are said to have or to be developing cyber military capabilities, including the five permanent member States of the UN Security Council.[8] Examples of the use of cyber operations

M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services", 14 February 2019, available at: www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf; Jeremy Fleming, GCHQ, "Director's Speech at CyberUK18", 12 April 2018, available at: www.gchq.gov.uk/pdfs/speech/director-cyber-uk-speech-2018.pdf.

3 "Hackers Interrupt Israeli Eurovision WebCast with Faked Explosions", *BBC News*, 15 May 2019, available at: www.bbc.co.uk/news/technology-48280902; Zak Doffman, "Israel Responds to Cyber Attack with an Air Strike on Cyber Attackers in World First", *Forbes*, 6 May 2019, available at: www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#1c692f73afb5. While the purported target of the alleged cyber operation by Hamas has not been publicly released, the targeting of Hamas' building by kinetic means was said to be based on intelligence gained as part of the Israeli Defence Forces' cyber defence effort.

4 David Hollis, "Cyberwar Case Study: Georgia 2008", *Small War Journal*, 2010, available at: https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

5 Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar", *Wired*, 20 June 2017, available at: www.wired.com/story/russian-hackers-attack-ukraine/; Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, 22 August 2018, available at: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

6 Blake Johnson *et al.*, "Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure", *Fireeye Blogs*, 14 December 2017, available at: www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

7 For example, there have been various media reports – based on anonymous official sources – that the United States has carried out cyber operations against targets in Russia and Iran, and that Israel has carried out a cyber operation against a port in Iran. See Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms", *Washington Post*, 27 February 2019, available at: https://tinyurl.com/yxs8twyv; David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid", *New York Times*, 15 June 2019, available at: www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; Julian E. Varnes and Thomas Gibbons-Neff, "U.S. Carried out Cyberattacks on Iran", *New York Times*, 22 June 2019, available at: www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; Joby Warrick and Ellen Nakashima, "Officials: Israel Linked to a Disruptive Cyberattack on Iranian Port Facility", *Washington Post*, 18 May 2020, available at: https://tinyurl.com/y4onsrt9. On so-called "grey zones" and cyber technology, see Camille Faure, "Utilisation contemporaine et future des technologies cyber/numériques dans les conflits armés", in Gabriella Venturini and Gian Luca Beruto (eds), *Whither the Human in Armed Conflict? IHL Implications of New Technology in Warfare*, 42nd Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2020 (forthcoming); Gary Corn, "Punching on the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses", *Just Security*, 11 February 2020, available at: www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/. On the threshold of application of IHL, see the section below entitled "Cyber Operations that Are Governed by IHL".

8 In addition to the United States and the United Kingdom, France has set out the objective of "acquir[ing] a cyber defence capability" to defend against "foreign States or terrorist groups [which] could attack the

during conflicts include espionage; target identification; information operations to affect the enemy's morale and will to fight; the interruption, deception or obfuscation of the enemy's communication systems aimed at hindering force coordination; and cyber operations in support of kinetic operations.[9] An example of the latter is the disabling of an enemy's military radar stations in support of air strikes.[10] Moreover, as seen in a range of cyber operations over the past decade – which may not necessarily have occurred in the context of armed conflicts – cyber operations against electricity grids, health-care systems, nuclear facilities or other critical infrastructure risk causing significant human harm.[11] Legally, discussions on whether and how international humanitarian law applies to, and restricts, cyber operations during armed conflicts began over two decades ago.[12] The drafting processes for the two *Tallinn Manuals on the International Law Applicable to Cyber Operations* (Tallinn Manuals) have shown that there is

critical infrastructures". France, Agence Nationale de la Sécurité des Système d'Information, *Information System Defence and Security: France's Strategy*, 2011, available at: www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf. The 2015 *White Paper on China's Military Strategy* states that "in response to the increasing development of cyber military capabilities from other states, China will develop a defensive cyber military capacity". See Government of China, *White Paper on China's Military Strategy*, 2015, available at: www.gov.cn/zhengce/2015-05/26/content_2868988.htm. Russia has been less explicit on the subject, but the Russian Federation's Doctrine of Information Security identifies "upgrading the information security system of the Armed Forces of the Russian Federation, other troops, military formations and bodies, including forces and means of information confrontation" as a "key area of ensuring information security in the field of national defence". See Ministry of Foreign Affairs of the Russian Federation, *Doctrine of Information Security of the Russian Federation*, 5 December 2016, available at: https://tinyurl.com/y6yhp7pv. See also Ministry of Defence of the Russian Federation, "Western MD Operators Repelled Cyberattack of the Simulated Enemy in the Course of the Union Shield – 2015", 2015, available at: https://eng.mil.ru/en/news_page/country/more.htm?id=12056193@egNews. For general estimates on the spread of cyber tools, see Anthony Craig, "Understanding the Proliferation of Cyber Capabilities", Council on Foreign Relations, 2018, available at: www.cfr.org/blog/understanding-proliferation-cyber-capabilities. According to the United Nations Institute for Disarmament Research (UNIDIR) Cyber Index, in 2012 forty-seven States had cyber security programmes that gave some role to their armed forces (UNIDIR, *The Cyber Index: International Security Trends and Realities*, UN Doc. UNIDIR/2013/3, Geneva, 2013, p. 1), while in 2020 Digital Watch Observatory recorded twenty-three and thirty States with respectively evidence or indications of offensive cyber capabilities (Digital Watch Observatory, "UN GGE and OEWG", available at: https://dig.watch/processes/un-gge).

9 ICRC, *Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts*, forthcoming.

10 Sharon Weinberger, "How Israel Spoofed Syria's Air Defense System", *Wired*, 4 October 2007, available at: www.wired.com/2007/10/how-israel-spoo/; Lewis Page, "Israeli Sky-Hack Switched Off Syrian Radars Countrywide", *The Register*, 22 November 2007, available at: www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion/.

11 In November 2018, the ICRC convened an expert meeting to develop a realistic assessment of cyber capabilities and their potential humanitarian consequences in light of their technical characteristics. See Laurent Gisel and Lukasz Olejnik (eds), *ICRC Expert Meeting: The Potential Human Cost of Cyber Operations*, ICRC, Geneva, 2019, available at: www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf. See also Sergio Caltagirone, "Industrial Cyber Attacks: A Humanitarian Crisis in the Making", *Humanitarian Law and Policy Blog*, 3 December 2019, available at: https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/. The World Economic Forum (WEF) *Global Risks Report 2020* ranks cyber attacks among the top ten risks in terms of both likelihood and impact; see WEF, *The Global Risks Report 2020*, 2020, p. 3, available at: www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.

12 See US Department of Defense Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, 1999, available at: https://fas.org/irp/eprint/io-legal.pdf; for one of the early academic examinations of these questions, see Knut Dörmann, "Computer Network Attack and

significant consensus among experts that IHL applies in cyberspace and that its basic rules and principles can and must be applied when conducting cyber operations during armed conflict.[13] As seen in the diverging views recorded in the Tallinn Manuals as well as in a growing number of State positions and the rich body of academic publications on cyber-related issues, however, various aspects of how certain rules of IHL apply in this field remain under-explored and disagreement exists on other questions, including some of the most-examined ones (see the section below on "The Limits that IHL Imposes on the use of Cyber Capabilities during Armed Conflicts"). At the political level, recent and ongoing discussions in the UN have shown that finding agreement on the applicability of IHL to cyber operations and furthering the study of how its rules should be interpreted remains challenging.[14] Discussions on questions relating to "information security" started when the Russian Federation introduced a first resolution on the subject at the UN General Assembly in 1998. These discussions have intensified over the course of the last few years. Since 2004, governmental experts have been meeting in six consecutive Groups of Governmental Experts on questions relating to information and telecommunications in the context of international security. In 2018, the UN General Assembly also established the OEWG, which runs in parallel to the GGEs. Both groups are mandated, *inter alia*, to study "how international law applies to the use of information and communications technologies by States".[15] These discussions should build on the important conclusions reached by previous GGEs. In 2013 and 2015, States in the GGE affirmed that "international law and in particular the Charter of the United Nations is applicable" in the information and communication technology environment and cited "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction".[16] Yet, it appears from recent discussions in these UN processes, and as discussed further below, that finding agreement on the applicability of IHL to cyber operations and furthering the study of how its rules should be interpreted is challenging.

International Humanitarian Law", 2001, available at: www.icrc.org/en/doc/resources/documents/article/other/5p2alj.htm.

13 See Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013 (Tallinn Manual); Michael N. Schmitt and Liis Vihul (eds), *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0).

14 See, notably, OEWG, "Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", 11 March 2020, available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

15 UNGA Res. 73/27, "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/73/27, 11 December 2018, para. 5; UNGA Res. 73/266, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", UN Doc. A/RES/73/266, 2 January 2019, para. 3.

16 UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General", UN Doc. A/70/174, 22 July 2015, paras 24, 28(d).

At the regional level, already in 2009 member States of the Shanghai Cooperation Organization (SCO) had identified "[d]eveloping and using information weapons" and "preparing and conducting information warfare" to be a major threat in the field of international information security, but they remained silent on the applicable legal framework.[17] Discussions on the application of international law, including IHL, have taken place in the Asian–African Legal Consultative Organization (AALCO) (which established an Open-Ended Working Group on International Law in Cyberspace in 2015)[18], the Commonwealth,[19] the European Union,[20] the North Atlantic Treaty Organization (NATO)[21] and the Organization of American States (OAS),[22] among others.

The potential human cost of cyber operations

The development of information and communication technology, including communication over computer networks (cyberspace), offers tremendous benefits and opportunities for States, societies and individuals in the social, economic, development, and information and communication realms, among others. The international community, societies, and each of us individually are increasingly relying on digital tools. This trend – which may be accelerated further by the COVID-19 pandemic spreading at the time of writing this article – increases our dependency on the uninterrupted functioning of these technologies, and thus increases our vulnerability to cyber operations. The rapidly evolving nature of cyberspace and cyber technology, and the potential human cost of cyber operations, therefore necessitates constant monitoring and assessment.

The use of cyber tools as a means or method of warfare offers militaries the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure. Depending on the circumstances, cyber operations might enable targeting a military objective while reducing the expected incidental damage to civilian objects compared to the use

17 Agreement on Cooperation in the Field of Ensuring International Information Security among Member States of the Shanghai Cooperation Organization, Yekaterinburg, 16 June 2009 (SCO Agreement); unofficial translation in Ministry of Defense of the Russian Federation, "The State and the Prospects of Russian Military Cooperation on International Information Security (A Collection of Papers)", 2014, pp. 77 ff. See also, for example, J. Fleming, above note 2, p. 5.

18 See AALCO, *International Law in Cyberspace*, Doc. No. AALCO/58/DAR ES SALAAM/2019/SD/17, available at: www.aalco.int/Final%20Cyberspace%202019.pdf.

19 See the Commonwealth Cyber Declaration issued at the Commonwealth Heads of Government Meeting, London, 16–20 April 2018, available at: https://thecommonwealth.org/commonwealth-cyber-declaration.

20 See, for example, EU Council Conclusions, General Affairs Council meeting, Doc. No. 11357/13, 25 June 2013.

21 See, for example, the Wales Summit Declaration issued by the heads of State and government participating in the meeting of NATO in Wales, 5 September 2014, para. 72, available at: www.nato.int/cps/en/natohq/official_texts_112964.htm.

22 See OAS, *Improving Transparency: International Law and State Cyber Operations: Fourth Report*, OAS Doc. CJI/doc. 603/20 rev.1 corr.1, 5 March 2020, available at: www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf.

of other means of warfare. In recent intergovernmental discussions, some States emphasized that if employed responsibly and in accordance with international law, "the use of ICTs [information and communications technologies] in military contexts may be preferable to use of kinetic weapons and can be de-escalatory".[23] In contrast, as noted above, SCO member States have warned of the dangers of "[d]eveloping and using information weapons" and "preparing and conducting information warfare".[24]

Conducting highly discriminative cyber operations that comply with IHL and spare civilian populations can be technologically challenging. The interconnectivity that characterizes cyberspace means that whatever has an interface with the Internet can be affected by cyber operations conducted from anywhere in the world. A cyber attack on a specific system may have repercussions on various other systems, regardless of where those systems are located. There is a real risk that cyber tools – either deliberately or by mistake – may cause large-scale and diverse effects on critical civilian infrastructure. The interconnectedness of cyberspace also means that all States should be concerned with its effective regulation: "attacks carried out against one State can affect many others – wherever they are located and irrespective of whether they are involved in the conflict".[25] Cyber operations conducted over recent years – primarily outside armed conflicts – have shown that malware can spread instantly around the globe and affect civilian infrastructure and the provision of essential services.[26] As a result, commentators are warning that industrial cyber attacks present "a humanitarian crisis in the making".[27]

The health-care sector seems particularly vulnerable to cyber attacks.[28] The sector is moving towards increased digitization and interconnectivity, which increases its digital dependency and its attack surface – a development that is likely to continue in the coming years. Too often, these developments have not been matched by a corresponding improvement in cyber security.[29]

23 "UK Response to Chair's Initial 'Pre-draft' of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security", available at: https://front.un-arm.org/wp-content/uploads/2020/04/20200415-oewg-predraft-uk.pdf. See also ICRC, above note 9; Gary Corn, "The Potential Human Costs of Eschewing Cyber Operations", *Humanitarian Law and Policy Blog*, 31 May 2019, available at: https://blogs.icrc.org/law-and-policy/2019/05/31/potential-human-costs-eschewing-cyber-operations/.

24 SCO Agreement, above note 17, Art. 2.

25 Helen Durham, "Cyber Operations during Armed Conflict: 7 Essential Law and Policy Questions", *Humanitarian Law and Policy Blog*, 26 March 2020, available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/.

26 Examples include the malware CrashOverride, the ransomware WannaCry, the wiper program NotPetya, and the malware Triton. CrashOverride affected the provision of electricity in Ukraine; WannaCry affected hospitals in several countries; NotPetya affected a very large number of businesses; Triton was aimed at disrupting industrial control systems, and was reportedly used in attacks against Saudi Arabian petrochemical plants. For some discussion, see Laurent Gisel and Lukasz Olejnik, "The Potential Human Cost of Cyber Operations: Starting the Conversation", *Humanitarian Law and Policy Blog*, 14 November 2018, available at: https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/.

27 See S. Caltagirone, above note 11.

28 L. Gisel and L. Olejnik (eds), above note 11, pp. 18–22.

This vulnerability became particularly apparent during the COVID-19 pandemic, when hospitals and other health-care facilities in various States had their operations disrupted by hostile cyber operations. In light of the particular importance of the health-care sector for mitigating suffering at all times, but especially during armed conflicts and health crises, the ICRC has called on all States to respect and protect medical services and medical facilities against cyber attacks of any kind, whether in time of peace or in time of conflict, and to reaffirm and recommit to international rules that prohibit such actions.[30] While this call reflects existing obligations under IHL as applicable to cyber operations during armed conflict,[31] it would reaffirm, or arguably strengthen, existing prohibitions under public international law that apply at all times.[32]

Cyber operations against other critical civilian infrastructure, such as electricity, water and sanitation, can also cause significant harm to humans.[33] This infrastructure is often operated by industrial control systems (ICSs). A cyber attack against an ICS requires specific expertise and sophistication, and often, custom-made malware. While ICS attacks have been less frequent than other types of cyber operations, their frequency is reportedly increasing and the severity of the threat has evolved more rapidly than anticipated only a few years ago.[34] Cyber security specialists have pointed out that "due to the potential of cyber-physical attacks to have kinetic effect and cause casualties, it is urgent and of utmost importance for the international community of IT security specialists,

29 See Aaron F. Brantly, "The Cybersecurity of Health", *Council on Foreign Relations Blog*, 8 April 2020, available at: https://tinyurl.com/yxc4oc9j.

30 See "Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector", *Humanitarian Law and Policy Blog*, 26 May 2020, available at: https://blogs.icrc.org/law-and-policy/2020/05/26/call-global-leaders-stop-cyberattacks-healthcare/. In the specific framework of the above-mentioned OEWG, the ICRC suggested that States could adopt a norm whereby they commit "not to conduct or knowingly support cyber operations that would harm medical services or medical facilities, and to take measures to protect medical services from harm". This suggestion combines a "negative" element, namely that States should not conduct or knowingly support cyber activity that would harm medical services or facilities, and a "positive" element, meaning that States should take measures to protect medical services from harm. See ICRC, "Norms for Responsible State Behavior on Cyber Operations Should Build on International Law", 11 February 2020, available at: www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-build-international-law.

31 See below section entitled "IHL Rules Protecting Objects Indispensable to the Survival of the Civilian Population, Medical Services, and Humanitarian Relief Operations".

32 For greater detail on how international law applies to such operations, see Kubo Mačák, Laurent Gisel and Tilman Rodenhäuser, "Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong are International Law Protections?", *Just Security*, 27 March 2020, available at: www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/. See also the Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care Sector, May 2020 (Oxford Statement), available at: www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea.

33 L. Gisel and L. Olejnik (eds), above note 11, pp. 23–28. See also Aron Heller, "Israeli Cyber Chief: Major Attack on Water Systems Thwarted", *ABC News*, 28 May 2020, available at: https://abcnews.go.com/International/wireStory/israeli-cyber-chief-major-attack-water-systems-thwarted-70920855.

34 *Ibid.*, p. 25.

governments and humanitarian lawyers to have a conversation about how to regulate the deployment of cyber-physical attacks".[35]

As will be discussed later on in this article, in an armed conflict IHL protects the health-care sector quite comprehensively, and it prohibits attacks on civilian infrastructure, unless such infrastructure has become a military objective.

Thinking beyond the impact of cyber operations on specific infrastructure, there are at least three characteristics of cyber operations that raise further concern.[36]

First, though not impossible, attributing cyber attacks to a State or non-State actor has proven challenging.[37] This hampers the possibility of identifying actors who violate IHL in cyberspace and holding them responsible, which is one way to ensure compliance with IHL. Plausible deniability, and the hope of remaining covered, may also alter the political calculations involved in conducting cyber attacks – and in conducting them in violation of international law.

Second, as noted for example by China, "the proliferation of malicious cyber tools and technology [is] rising".[38] Cyber tools and methods can indeed proliferate in a unique manner that is difficult to control. Today, sophisticated cyber attacks are only carried out by the most advanced and best-resourced actors. Once malware is used, stolen, leaked or otherwise becomes available, however, actors other than those who developed the malware might be able to find it online, reverse engineer it, and reuse it for their own purposes.

Third, cyber operations bear a risk of overreaction by targeted States and a subsequent escalation in violence. For the target of a cyber attack, it is normally difficult to know whether the attacker aims at espionage or at causing other, potentially physical damage. The aim of a cyber operation may only be identified with certainty once the effect or the end goal is achieved. Hence, there is a risk that the target of an operation will anticipate worst-case impact and react in a stronger manner than if it knew that the attacker's intent was solely espionage.

At the time of writing, cyber operations have not caused major human harm. However, significant economic harm has been caused.[39] With regard to the

35 Marina Krotofil, "Casualties Caused through Computer Network Attacks: The Potential Human Costs of Cyber Warfare", 42nd Round Table on Current Issues of International Humanitarian Law, 2019, available at: http://iihl.org/wp-content/uploads/2019/11/Krotofil1.pdf.

36 See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, 2019 (ICRC Challenges Report 2019), p. 27, available at: www.icrc.org/en/document/icrc-report-ihl-and-challenges-contemporary-armed-conflicts; L. Gisel and L. Olejnik (eds), above note 11, p. 7.

37 For a broader discussion on attribution, including the pertinent international law rules, see the section below entitled "The Issue of Attribution".

38 Statement by Counsellor Sun Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UN General Assembly, 23 October 2017, available at: www.china-un.org/eng/chinaandun/disarmament_armscontrol/unga/t1505683.htm.

39 The overall cost of cyber crime alone is measured in trillions of dollars: it was estimated at $3 trillion in 2015 worldwide, and this figure is predicted to double by 2021 (Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation", Herjavec Group, 17 August 2016, available at: www.herjavecgroup.com/hackerpocalypse-cybercrime-report/). NotPetya's impact was estimated at well above $1 billion, with some estimates as high at $10 billion (Fred O'Connor, "NotPetya Still Roils Company's Finances,

potential human cost of cyber operations, much is unknown in terms of technological evolution, the capabilities and the tools developed by the most sophisticated actors – including military ones – and the extent to which the use of cyber operations during armed conflicts might be different from the trends observed so far. In other words, while the risk of human cost does not appear extremely high based on current observations, especially considering the destruction and suffering that conflicts always cause, the evolution of cyber operations requires close attention due to existing uncertainties and the rapid pace of change.

The applicability of IHL to cyber operations during armed conflicts

From a legal point of view, the primary framework imposing limitations on the use of cyber operations during armed conflict and protecting civilian populations against potential harm is international humanitarian law.

IHL does not contain a definition of cyber operations, cyber warfare or cyber war, and neither do other fields of international law. Various definitions of cyber operations have been used in military or other documents by certain States.[40] Other States refer instead to information warfare or information war and define this notion in a manner that includes at least some aspects of what is often understood as cyber warfare.[41] Irrespective of how cyber operations, cyber warfare or information warfare are defined by States and others, the determination of whether IHL applies to such operations has to be made based on the nature, effects and circumstances of such operations.

The ICRC understands "cyber operations during armed conflict" to mean operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict.[42]

Costing Organizations $1.2 Billion in Revenue", *Cybereason*, 9 November 2017, available at: www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue; A. Greenberg, above note 5). The financial system is also often affected by cyber attacks: see, for example, Choe Sang-Hun, "Computer Networks in South Korea Are Paralyzed in Cyberattacks", *New York Times*, 20 March 2013, available at: www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html.

40 See, for instance, US Department of Defense, *DOD Dictionary of Military and Associated Terms*.

41 The SCO Agreement, above note 17, defines "information war" as "a confrontation between two or more States in the information space with the aim of damaging information systems, processes and resources, critically important and other structures, undermining political, economic and social systems, psychologically manipulating masses of the population to destabilize society and the State, and also forcing the State to take decisions in the interest of the opposing party". The Russian Federation Armed Forces define information war in the same manner, stating that "the Armed Forces of the Russian Federation follow … international humanitarian law" during military activities in the global information space (Ministry of Defence of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept*, 2011, section 2.1, available at: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle).

42 See ICRC, above note 1.

While there continues to be debate on the question of whether IHL applies to, and therefore restricts, cyber operations during armed conflict, from the outset the ICRC has taken a clear and affirmative position.[43] In the ICRC's view, there is no question that cyber operations during armed conflicts, or cyber warfare, are regulated by IHL – just as is any weapon, means or method of warfare used by a belligerent in a conflict, whether new or old. The fact that cyber operations rely on new and continuously developing technology does not prevent the application of IHL to the use of such technologies as means or methods of warfare. This holds true whether cyberspace is considered as a new domain of warfare similar to air, land, sea and outer space; as a different type of domain because it is man-made while the former are natural; or not as a domain as such.

In our view, there is cogent support for this view in IHL treaties, in the jurisprudence of the International Court of Justice (ICJ), and in the views expressed by a number of States and international organizations.

The very object and purpose of IHL is to regulate future conflicts, meaning those that occur after the adoption of an IHL treaty. When adopting IHL treaties, States included norms that anticipate the development of new means and methods of warfare and presumed that IHL will apply to them. Already in 1868, the St Petersburg Declaration intended that the principles it established should be maintained with respect to "future improvements which science may effect in the armament of troops".[44] An important and more recent IHL rule in this respect is found in Article 36 of the 1977 Additional Protocol I (AP I),[45] which states:

> In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.

Undoubtedly, this obligation is based on the assumption that IHL applies to such new weapons, means and methods – otherwise, it would not be necessary to review their lawfulness under existing law. This includes weapons, means and methods of warfare that rely on cyber technology.

The conclusion that IHL applies to cyber operations during armed conflict finds further support in the views expressed by the ICJ. In its Advisory Opinion on the legality of the threat or use of nuclear weapons, the Court recalled that the established principles and rules of humanitarian law applicable in armed conflict apply "to all forms of warfare and to all kinds of weapons", including "those of

43 See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, 2011 (ICRC Challenges Report 2011), pp. 36–39, available at: www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf; K. Dörmann, above note 12.

44 Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, St Petersburg, 29 November/11 December 1868.

45 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978).

the future".[46] Again, this includes cyber operations. This view is also widely recognized among experts.[47]

There is increasing recognition among States that international law applies in cyberspace, and in particular that IHL applies to, and therefore restricts, cyber operations during armed conflicts. As mentioned above, in the 2013 and 2015 reports of the UN GGE, experts concluded that "international law, and in particular the Charter of the United Nations, is applicable" in the information and communication technologies environment,[48] a conclusion that has been first welcomed[49] and then confirmed[50] by the UN General Assembly. The 2015 report also cited "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction".[51] While this list of principles does not mention IHL explicitly, commentators have pointed out that these are "IHL's core principles".[52]

In line with this conclusion, an increasing number of States and international organizations have publicly asserted that IHL applies to cyber operations during armed conflict. This includes, for example, the EU[53] and NATO.[54] Moreover, the Paris Call for Trust and Security in Cyberspace (supported by seventy-eight States as of April 2020) has reaffirmed the applicability of IHL to cyber operations during armed conflict;[55] the heads of government of the 54 Commonwealth States have "[c]ommit[ted] to move forward discussions on how … applicable international humanitarian law, applies in cyberspace in all its aspects";[56] and States' responses to a study conducted by

46 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, para. 86.

47 See Tallinn Manual 2.0, above note 13, Rule 80; Oxford Statement, above note 32, point 5. Also see the article by Zhixiong Huang and Yaohui Ying in this issue of the *Review*; and see Ma Xinmin, at the time deputy director-general of the Department of Treaty and Law, Ministry of Foreign Affairs of the People's Republic of China, writing in a personal capacity: "[T]he scope of applicability of the rules of IHL has been expanded. … [I]t has also been broadened to cyberspace. The UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security confirmed in its 2013 and 2015 reports that international law, particularly the UN Charter, is applicable in cyberspace. IHL should, therefore, in principle be applicable to cyber attacks, but how to apply it is still open to discussion" (unofficial and informal translation). Ma Xinmin, "International Humanitarian Law in Flux: Development and New Agendas – In Commemoration of the 40th Anniversary of the 1977 Adoption Protocols to the Geneva Conventions", *Chinese Review of International Law*, Vol. 30, No. 4, 2017, p. 8.

48 UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General", UN Doc. A/68/98, 24 June 2013, para. 19, and UN Doc. A/70/174, 22 July 2015, para. 24.

49 UNGA Res. 70/237, "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/70/237, 30 December 2015, preambular para. 16.

50 UNGA Res. 73/27, above note 15, preambular para. 17; UNGA Res. 73/266, above note 15, preambular para. 12.

51 UN Doc. A/70/174, above note 48, para. 28(d).

52 Michael N. Schmitt, "France Speaks Out on IHL and Cyber Operations: Part I", *EJIL: Talk!*, 30 September 2019, available at: www.ejiltalk.org/france-speaks-out-on-ihl-and-cyber-operations-part-i/.

53 EU Council Conclusions, above note 20.

54 Wales Summit Declaration, above note 21, para. 72.

55 See "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace", *France Diplomacy*, available at: www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

56 Commonwealth Cyber Declaration, above note 19, p. 4, para. 4.

the OAS Juridical Committee have "reveal[ed] support for the applicability of IHL" in cyberspace.[57]

At the same time, in the context of discussions on the applicability of IHL to cyber operations during armed conflict, a number of States have expressed opposition to the militarization of cyberspace, or a cyber arms race. States have also expressed concerns regarding a possible legitimization of the use of military cyber operations,[58] called for prudence in the discussion of the applicability of IHL,[59] and noted that IHL "must apply taking note of the peculiarities of cyber warfare".[60] These are important considerations, but they should not be understood as being incompatible with the application of IHL to cyber operations during armed conflict.

In our view, however, asserting that IHL applies to cyber operations during armed conflict is not an encouragement to militarize cyberspace and should not, in

57 See OAS, above note 22, para. 43 (mentioning Bolivia, Chile, Guyana, Peru and the United States); Ecuador's response may appear to have implied such support (see also paras 19–21, 25). Other member States of the OAS expressed this position in the context of the OEWG. See comments by Brazil, Colombia and Uruguay on the initial pre-draft of the OEWG report, available at: www.un.org/disarmament/open-ended-working-group/. See, however, the views of Cuba, Nicaragua and Venezuela, who note, among other things, that there is not yet consensus on the applicability of IHL in cyberspace and that direct reference to IHL in the report may validate or legitimize the militarization of cyberspace.

58 See, most recently, the submissions of China, Cuba, Iran, Nicaragua, Russia and others on the initial pre-draft of the OEWG report, available at: www.un.org/disarmament/open-ended-working-group/. See also, for example, People's Republic of China, *Position Paper of the People's Republic of China for the 73rd Session of the United Nations General Assembly*, 2018, p. 10, available at: https://tinyurl.com/y4qquywp; "Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 23 June 2017, p. 2; Ministry of Foreign Affairs of the Russian Federation, "Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere", 29 June 2017.

59 "The applicability of the law of armed conflicts and *jus ad bellum* needs to be handled with prudence. The lawfulness of cyber war should not be recognized under any circumstance. States should not turn cyberspace into a new battlefield": "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", September 2019, p. 6, available at: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf. "We should be extremely cautious against any attempt to introduce use of force in any form into cyberspace, have sober assessment on possible conflicts and confrontations resulted from the indiscriminate application of the law of armed conflicts in cyberspace, and refrain from sending wrong messages to the world": "China's Contribution to the Initial Pre-Draft of OEWG Report", April 2020, p. 5, available at: https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf. "[W]ithout state practice, we should be very prudent on the discussion of application of humanitarian law in so called 'cyber wars.' The reason is very simple but fundamental: firstly, no cyber wars shall be permitted; and secondly, cyber war will be a totally new form of high-tech war": China statement at AALCO 58th Annual Session, in AALCO, *Verbatim Record of Discussions: Fifty-Eighth Annual Session*, Doc No. AALCO/58/DAR ES SALAAM/2019/VR, 2019, p. 176, available at: www.aalco.int/Verbatim%20(FINAL)%2020200311.pdf.

60 China has stated at a meeting of the AALCO Working Group on International Law in Cyberspace that "the regimes of *jus ad bellum* and *jus in bello* must apply taking note of the peculiarities of cyber warfare". AALCO, *Summary Report of the Fourth Meeting of the Open-Ended Working Group on International Law in Cyberspace*, 3 September 2019, available at: www.aalco.int/Summary%20Report%20as%20Adopted.pdf.

any way, be understood as legitimizing cyber warfare.[61] Any resort to force by States, whether cyber or kinetic in nature, always remains governed by the UN Charter and customary international law, in particular the prohibition against the use of force.[62] International disputes must be settled by peaceful means. This principle applies in cyberspace as in all other domains. In addition to – and independent of – the requirements of the UN Charter, IHL provides limits on the conduct of hostilities if and when States or non-State parties chose to resort to cyber operations during armed conflict. In particular, IHL protects civilians and civilian objects from the effects of hostilities by restricting the belligerents' choice of means and methods of warfare, independent of whether or not the use of force was lawful. This means that instead of legitimizing cyber operations (or any other military operation) during armed conflict, IHL – the *jus in bello* – provides limits in addition to those found in the UN Charter and customary international law – the *jus ad bellum*. Furthermore, IHL actually imposes some limits on the militarization of cyberspace. For example, it prohibits the development of cyber capabilities that would qualify as weapons and would be indiscriminate by nature or would be of a nature to cause superfluous injury or unnecessary suffering.[63]

If it is accepted that IHL applies to cyber operations during armed conflicts generally, the subsequent question is whether all or only some rules of IHL apply. In this respect, the scope of application of IHL rules regulating means and methods of warfare may be broadly divided into rules that apply to all weapons, means and methods of warfare, wherever they are used (such as the principles of distinction, proportionality and precaution), and rules that are specific to certain weapons (such as weapons treaties) or certain domains (such as rules specifically regulating naval warfare). All the main customary principles and rules regulating the conduct of hostilities belong to the first category and do apply to cyber operations during armed conflict.[64] In contrast, a more detailed analysis will be required regarding the applicability of IHL rules that are specific to certain weapons or certain domains.

The fact that IHL applies does not prevent States from developing international law further, agreeing on voluntary norms, or working towards common interpretations of existing rules. For instance, when it established a UN OEWG in 2018, a majority of States in the UN General Assembly "welcome[d]" a set of "international rules, norms and principles of responsible behaviour of States" that build on the norms that were developed over the years by the UN GGEs.[65] Another example of possible new rules in the field of information

61 This view has also been expressed in, among others, the submissions of Australia, Brazil, Chile, Denmark and the United Kingdom on the initial pre-draft of the OEWG report, available at: www.un.org/disarmament/open-ended-working-group/.

62 UN Charter, Art. 2(4).

63 See Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rules 70, 71, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul.

64 The principles and rules regulating the conduct of hostilities are highlighted further below, under the section entitled "The Limits that IHL Imposes on the Use of Cyber Capabilities during Armed Conflicts".

65 UNGA Res. 73/27, above note 15.

security is included in the International Code of Conduct for Information Security, submitted in 2011 to the UN by the member States of the SCO. Under the Code, States would pledge, *inter alia*, "not to proliferate information weapons and related technologies".[66] There are also academic suggestions, including with regard to further legal or policy restrictions on cyber operations during armed conflicts.[67]

To sum up, while cogent legal reasons and increasing international support exist for the conclusion that IHL applies to cyber operations during armed conflict, the issue does not enjoy universal agreement yet. As has been shown in this section, however, a careful examination of the various arguments raised in multilateral discussions shows that affirming IHL applicability does not legitimize either the militarization of cyberspace or the use of malicious cyber operations. Moreover, it does not preclude the development of possible new rules but rather provides a fundamental legal framework that possible new rules could – and should – build on.

Can cyber operations alone cross "the threshold"? Clarifying the difference between the relevant thresholds under IHL and the UN Charter

In light of the manifold cyber operations that are reported on a daily basis, it is important to recall that IHL only applies to cyber operations that form part of an armed conflict otherwise waged with traditional weapons, or, less likely, cyber operations that alone amount to an armed conflict in the absence of kinetic operations. As underlined in the previous section, the question of whether IHL applies to cyber operations during armed conflicts must be analyzed separately from that of whether there has been a violation of the rules governing the use of force under the UN Charter. In the context of the application of IHL and of the UN Charter, a key issue is the attribution of cyber operations to States. These

66 The proposed International Code of Conduct for Information Security is available at: http://nz.chineseembassy.org/eng/zgyw/t858978.htm. It was submitted by China, Russia, Tajikistan and Uzbekistan in 2011, and co-sponsored by Kazakhstan and Kyrgyzstan in 2013 (see UN Doc. A/68/98, above note 48, p. 8, para. 18). Similarly, in 2011 the Ministry of Foreign Affairs of the Russian Federation presented a draft Convention on International Information Security (22 September 2011, available at: www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666) which lists among the "Main Measures for Averting Military Conflict in the Information Space" that States shall "take action aimed at limiting the proliferation of 'information weapons' and the technology for their creation" (Art. 6(10)). Its Article 7(2) also foresees that "[i]n any international conflict, the right of the States Parties that are involved in the conflict to choose the means of 'information warfare' is limited by applicable norms of international humanitarian law".

67 Among many others, Pascucci, for instance, has suggested that the negotiation of an Additional Protocol IV could enable some of the issues raised by the application of the principle of distinction and proportionality in cyberspace to be addressed: Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution", *Minnesota Journal of International Law*, Vol. 26, No. 2, 2017. Schmitt, meanwhile, has put forward proposals in terms of policies that States could adopt: Michael N. Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations", *International Review of the Red Cross*, Vol. 101, No. 910, 2019, pp 333–355.

three points – which cyber operations are governed by IHL,[68] the relationship between IHL and the UN Charter, and questions of attribution – are addressed in this section.

Cyber operations that are governed by IHL

When cyber operations are conducted in the context of – and have a nexus to – an existing international or non-international armed conflict carried out through kinetic means, relevant IHL rules apply to, and regulate the conduct of, all parties to the conflict.[69] Cyber operations alongside, and in support of, kinetic operations during armed conflicts are the only type of operations that States have acknowledged and have considered to be governed by IHL.[70]

A separate question is whether cyber operations alone – absent kinetic operations – may be regulated by IHL. In other words, can a cyber operation be the first, and possibly only, shot in an armed conflict as defined by IHL? This is to be assessed according to Articles 2 and 3 common to the four Geneva Conventions of 1949[71] for international and non-international armed conflicts respectively.[72] These two types of armed conflict differ in the nature of the parties they involve, the intensity of violence that triggers the applicability of IHL, and some of the IHL rules that apply.

With regard to international armed conflicts, common Article 2 states that "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". It is today agreed that "an armed conflict exists whenever there is 'a resort to armed force between States'".[73] With regard to the question of whether there is a threshold of intensity with regard to international armed conflicts, there is some State practice,

68 For an illustration of these debates, see "Scenario 13: Cyber Operations as a Trigger of the Law of Armed Conflict", in Kubo Mačák, Tomáš Minárik and Taťána Jančárková (eds), *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/.

69 See ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed., Geneva, 2016 (ICRC Commentary on GC I), para. 254; Tallinn Manual 2.0, above note 13, Rule 80.

70 See references in note 2 above.

71 Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950) (GC I); Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950) (GC II); Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950) (GC III); Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) (GC IV).

72 Common Article 2(1): "[T]he 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." Common Article 3(1): "In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties …"

73 International Criminal Tribunal for the former Yugoslavia (ICTY), *The Prosecutor v. Duško Tadić*, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para. 70; ICRC Commentary on GC I, above note 69, para. 218.

and some strong humanitarian and conceptual arguments, that IHL applies as soon as armed force is used between States, irrespective of the intensity of the violence. IHL is primarily concerned with the protection of persons affected by armed conflict. Thus, as soon as they use armed force, States must direct their attacks at military objectives and not at civilians or civilian objects, and must take constant care to spare the latter. It cannot matter whether there is one or many civilians needing protection against attack.[74] At least where the use of cyber operations between States leads to effects akin to those of more traditional means and methods of warfare, IHL applies.

Experts generally agree that cyber operations, on their own, have the potential to cross the threshold of an international armed conflict under IHL.[75] The ICRC shares this view.[76] In a rare expression of a State's position on the issue, France has stated that "[c]yberoperations that constitute hostilities between two or more States may characterise the existence of international armed conflict".[77]

The question of exactly where this threshold lies remains unsettled.[78] In the ICRC's view, there is no reason to treat one or more cyber operations resulting in the destruction of civilian or military assets, or in the death or injury of soldiers or civilians, differently from equivalent attacks conducted through more traditional means and methods of warfare. Cyber operations might, however, also disable objects without physically damaging them. It remains to be seen if and under what conditions States might consider such operations to amount to a resort to armed force as understood in IHL, and therefore to be governed by this body of law.[79]

With regard to non-international armed conflicts, situations of internal violence may amount to a non-international armed conflict if there is "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".[80] The two criteria that derive from this definition – the organization of the parties to the conflict and the intensity of the violence – pose various questions regarding cyber operations. First, while State armed forces satisfy the organization criterion, determining the degree of

74 Similarly, if the resort to armed force leads, for example, to injuries or the capture of a member of another State's armed forces, IHL rules on the protection of the wounded and sick or the status and treatment of prisoners of war are relevant whether there is one or many prisoners, one or many wounded to be cared for. See ICRC Commentary on GC I, above note 69, paras 236–244.

75 Tallinn Manual 2.0, above note 13, Rule 82, para. 16.

76 ICRC Commentary on GC I, above note 69, paras 253–256.

77 French Ministry of the Armies, *International Law Applied to Operations in Cyberspace*, 2019, p. 12, available at: www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. This document specifies that "[w]hile an armed conflict consisting exclusively of digital activities cannot be ruled out in principle, it is based on the capacity of autonomous cyberoperations to reach the threshold of violence required to be categorised as such".

78 Tallinn Manual 2.0, above note 13, Rule 82, paras 11–16; as can be seen from paras 12–13, the question is not fully settled for kinetic operations either, and this uncertainty will permeate the debate on whether cyber operations alone can cross the threshold of an international armed conflict beyond the cyber-specific issues.

79 ICRC Commentary on GC I, above note 69, para. 255; Tallinn Manual 2.0, above note 13, Rule 82, para. 11.

80 ICTY, *Tadić*, above note 73, para. 70.

organization of an armed group is a more complicated and fact-specific assessment; it becomes all the more challenging – yet arguably not impossible – when that group is only organized online.[81] Second, unlike IHL applicable to international armed conflicts, which governs any resort to armed force between States regardless of its intensity,[82] a non-international armed conflict will only exist if violence between two or more organized parties is sufficiently intense. Again, while arguably not impossible in exceptional circumstances, it will be unlikely that cyber operations alone would meet the intensity requirement for a non-international armed conflict.[83] While expressing the view that prolonged cyber operations may in principle and depending on the circumstances constitute a non-international armed conflict, France held that the state of technology seems to rule out this possibility for the time being.[84]

It has rightly been emphasized that the law of armed conflict "does not regulate cyber operations that fall outside of an armed conflict situation".[85] Diverging views exist, however, on whether some or all of its principles should be applied, as a matter of policy, to cyber operations at all times.

The United States has recently stated that "even if the law of war does not technically apply because the proposed military cyber operation would not take place in the context of armed conflict, [the Department of Defense] nonetheless applies law-of-war principles"[86] as it does more generally with regard to all its operations.[87] In contrast, Russia has cautioned against "potentially dangerous … attempts to impose the principle of full and automatic applicability of IHL to the ICT environment in peacetime".[88]

81 ICRC Commentary on GC I, above note 69, para. 437; Tallinn Manual 2.0, above note 13, Rule 83, paras 13–15. For an in-depth analysis of the issue, see Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law*, Oxford University Press, Oxford, 2018, pp. 104–108.

82 ICRC Commentary on GC I, above note 69, paras 236–244.

83 *Ibid.*, para. 437. For further discussion, see Tallinn Manual 2.0, above note 13, Rule 83, paras 7–10; Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, p. 551; Michael N. Schmitt, "Classification of Cyber Conflict", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 260.

84 French Ministry of the Armies, above note 77, p. 12.

85 New Zealand Defence Force, *Manual of Armed Forces Law*, Vol. 4: *Law of Armed Conflict*, 2nd ed., DM 69, 2017 (New Zealand Military Manual), para. 5.2.23, available at: www.nzdf.mil.nz/assets/Publications/DM-69-2ed-vol4.pdf.

86 Paul C. Ney Jr., US Department of Defence General Counsel, Remarks at US Cyber Command Legal Conference, 2 March 2020, available at: www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

87 See US Department of Defense (DoD), Directive 2311.01E, "DoD Law of War Program", 2006 (amended 2011), paras 4–4.1: "It is DoD policy that … [m]embers of the DoD Components comply with the law of war during all armed conflicts, however such conflicts are characterized, *and in all other military operations*" (emphasis added). See also US Department of Defense (DoD), *Law of War Manual*, 2015 (DoD Law of War Manual), para. 3.1.1.2, available at: https://tinyurl.com/y6f7chxo.

88 Russia, "Commentary of the Russian Federation on the Initial 'Pre-draft' of the Final Report of the United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", April 2020, available at: https://front.un-arm.org/wp-content/uploads/2020/04/russian-commentary-on-oweg-zero-draft-report-eng.pdf.

While policy debates on this question are likely to continue, from a legal point of view it is undisputed that IHL does not apply outside the context of an armed conflict. It is true that some rules of IHL, such as the protection of persons not or no longer taking part in hostilities enshrined in common Article 3, or the strong protection of health-care facilities or objects indispensable to the survival of the civilian population, could have positive effects if applied at all times. In contrast, it may be more problematic to apply other IHL rules outside armed conflict, notably those derived from the principles of distinction and proportionality. These rules are based on the premise that attacks against military objectives are lawful under IHL during armed conflict. However, outside armed conflict, the notion of "military objectives" that may lawfully be attacked does not exist – even attacks against another State's military are prohibited. While the principle of proportionality also exists outside of armed conflict, it has a distinct meaning under other bodies of law and therefore operates differently during and outside armed conflicts.[89] Outside armed conflict, disputes among States and the use of force are solely regulated by other fields of international law, such as the UN Charter and human rights law, as applicable.

The relationship between IHL and the UN Charter

A State that considers carrying out a cyber operation against another State must analyze the lawfulness of such an operation under the *jus ad bellum* framework (as found in the UN Charter and customary international law) and the *jus in bello* framework (IHL). The UN Charter and IHL are complementary when it comes to the protection of humans from war and its effects, even though they are distinct fields of international law. Their objectives are complementary: while the preamble of the UN Charter states that it aims to "save succeeding generations from the scourge of war", the preamble of AP I states that the objective of IHL is "protecting the victims of armed conflict". Concretely, the UN Charter prohibits the use of force other than in self-defence or when authorized by the Security Council. The applicability of IHL does not replace or set aside the essential rules of the UN Charter, but if an armed conflict breaks out, IHL defines protections for those who do not (civilians) or no longer (for example, wounded soldiers or detainees) participate in hostilities and limits the belligerents' choice in the means and methods of warfare. Thus, while the UN Charter sets out – subject to narrow exceptions – a prohibition against the use of force, IHL imposes limits on how hostilities may be conducted once a conflict breaks out.

At the same time, IHL and the UN Charter are different fields of international law, each having its own concepts and terminology. As both are concerned with regulating the use of force, some of the terminology they use is similar and at times confusing. This is the case, for example, as regards the notion of "resort to armed force between States" to classify a conflict under IHL, and the prohibition against "the threat or use of force" and the right to self-

89 For a brief assessment, see ICRC Challenges Report 2019, above note 36, pp. 18–22.

defence against an "armed attack" under the UN Charter. While international law treaties do not define these notions – neither in general nor as regards cyberspace – certain basic elements can be distilled from jurisprudence and commentary.

As discussed above, IHL applies as soon as there is a resort to armed force between States, irrespective of the intensity of the violence.

The UN Charter does not define the term "use of force" under Article 2(4), and the question of what type of force may qualify remains subject to debate. Following the provision's drafting history and subsequent State practice, it may be concluded that the use of political or economic coercion is not included in this notion.[90] Instead, it has been argued that the prohibition against the use of force under the UN Charter is "limited to armed force".[91] Importantly with regard to cyber operations, the ICJ has stated that Article 2(4) prohibits "any use of force, regardless of the weapons employed".[92] Based on this finding, some States have emphasized that "crossing the threshold of the use of force depends not on the digital means employed but on the effects of the cyberoperation", and have concluded accordingly that a "cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons".[93] A number of examples given by States of the use of force in cyberspace seem to reflect this understanding, such as cyber operations causing injury or death of persons or damage to or destruction of property;[94] triggering a nuclear plant meltdown; opening a dam above a populated area, causing destruction; disabling air traffic control services, resulting in airplane crashes; and crippling a military's logistics systems.[95] Some States seem to interpret the prohibition against the use of force even more broadly, stating that it cannot be ruled out that "a cyberoperation without physical effects may also be characterised as a use of force",[96] or that "a cyber operation with a very serious financial or economic impact may qualify as the use of force".[97]

90 See Oliver Dörr and Albrecht Randelzhofer, "Article 2(4)", in Bruno Simma *et al.* (eds), *The Charter of the United Nations: A Commentary*, Vol. 1, Oxford University Press, Oxford, 2016, paras 17–20 of the commentary on Art. 2(4). Accordingly, experts have concluded that "neither non-destructive cyber psychological operations intended solely to undermine confidence in a government, nor a State's prohibition of e-commerce with another State designed to cause negative economic consequences, qualify as uses of force": Tallinn Manual 2.0, above note 13, para. 3 of the commentary on Rule 69.

91 O. Dörr and A. Randelzhofer, above note 90, p. 208, para. 16.

92 ICJ, above note 46, para. 39.

93 French Ministry of the Armies, above note 77, p. 7. See also Tallinn Manual 2.0, above note 13, para. 1 of the commentary on Rule 69.

94 See Estonia, "President of the Republic at the Opening of CyCon 2019", 29 May 2019, available at: www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html. Australian Department of Foreign Affairs and Trade, "Australia's International Cyber Engagement Strategy", 2019, available at: www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

95 DoD Law of War Manual, above note 87, para. 16.3.1.

96 French Ministry of the Armies, above note 77, p. 7. Examples that France provides of actions that could "be deemed uses of force" are "penetrating military systems in order to compromise French defence capabilities, or financing or even training individuals to carry out cyberattacks against France".

97 Dutch Ministry of Foreign Affairs, "Letter to the Parliament on the International Legal Order in Cyberspace", 5 July 2019, p. 4, available at: www.government.nl/ministries/ministry-of-foreign-affairs/

Turning to the right to self-defence under the UN Charter and customary international law, this right may only be exercised against an "armed attack". Following the ICJ's finding that only "the most grave forms of the use of force" may qualify as armed attacks and that such attacks must reach certain "scale and effects",[98] it may be concluded that a use of force must reach a certain intensity to qualify as an "armed attack".[99] Again, experts have held that "some cyber operations may be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter",[100] notably those whose effects are comparable to more traditional armed attacks. This view is also reflected in the public positions of some States.[101]

The questions of how the thresholds of a resort to armed force to which IHL applies, the prohibition of the use of force under the UN Charter, and the notion of "armed attacks" giving rise to the inherent right to self-defence are interpreted in cyberspace are evolving. While certain signposts may be identified based on the jurisprudence of the ICJ, the case law of international criminal tribunals and courts, State practice, and expert views, many issues remain blurred for the moment.

Nonetheless, it is important to emphasize that these three notions and concepts stem from different bodies of international law and have different meanings. As noted above, in the ICRC's view, a cyber operation that amounts to a resort to armed force between States under IHL is governed by that body of law even in the absence of a pre-existing armed conflict. In practice, such an operation may also amount to a prohibited use of force under the UN Charter. However, the two conclusions require a separate legal analysis: concluding that the threshold has been reached under one body of law does not necessarily preclude reaching a different conclusion under the other body of law. This is especially important when differentiating the applicability of IHL from the right to self-defence under the UN Charter. In view of the position that only the gravest forms of the use of force – meaning those that reach a certain scale and effects – may qualify as armed attacks, it is clear that not every resort to armed force to which IHL applies amounts to an armed attack under the UN Charter triggering the right to self-defence.[102] These differences have significant legal and practical consequences. Therefore, any analysis of a situation in which a State uses cyber operations against another State needs to distinguish the various notions and not merge them into one unspecified "threshold".

documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; French Ministry of the Armies, above note 77, p. 7. For a recent overview of States' positions, see Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, Policy Brief, Hague Program for Cyber Norms, 2020. For an illustration of these debates, see, for example, Kenneth Kraszewski, "Scenario 14: Ransomware Campaign", in K. Mačák, T. Minárik and T. Jančárková (eds), above note 68, paras L5–L13.

98 ICJ, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment, 27 June 1986, paras 191, 195.

99 This view is not, however, accepted by all States. For instance, the United States considers that any use of force is an armed attack.

100 Tallinn Manual 2.0, above note 13, para. 4 of the commentary on Rule 71.

101 Dutch Ministry of Foreign Affairs, above note 97, p. 4; French Ministry of the Armies, above note 77, p. 7.

102 H. Durham, above note 25.

The issue of attribution

In warfare generally – and in cyberspace in particular – States will at times use non-State actors, such as non-State armed groups or private military and security companies, to carry out certain acts, including cyber operations. The specific characteristics of cyberspace, such as the variety of possibilities for actors to hide or falsify their identity, complicate the attribution of conduct to specific individuals, and to parties to armed conflicts.[103] This raises important challenges when determining the applicability of IHL in a particular situation. If the perpetrator of a given operation – and thus the link between the operation and an armed conflict – cannot be identified, it is extremely difficult to determine whether IHL is even applicable to the operation.[104] First, as discussed above, different thresholds of violence are relevant to qualify State or non-State cyber attacks as an armed conflict. Thus, if the State or non-State origin of a cyber operation outside an ongoing armed conflict is not known, it is unclear which threshold applies. Second, even when an armed conflict is taking place, cyber attacks that have no nexus to the conflict (such as criminal acts unrelated to the conflict) are not regulated by IHL, and the inability to identify the author of a cyber operation might hamper the determination of whether such a nexus to the conflict exists. These examples show that determining who the author of a cyber operation is, and whether the operation can be attributed to a State or non-State party to the conflict, has important legal consequences.

Attribution of cyber operations is also important to ensure that actors who violate international law, including IHL, can be held accountable. The perception that it will be easier to deny responsibility for unlawful attacks may also weaken the taboo against such uses – and may make actors less scrupulous about conducting operations in violation of international law.[105]

This being said, attribution is not a problem from the perspective of the actors who conduct, direct or control cyber operations: they have all the facts at hand to determine under which international legal framework they are operating and which obligations they must respect.[106]

Under international law, a State is responsible for conduct attributable to it, including possible violations of IHL. This includes:

(a) violations committed by its organs, including its armed forces;
(b) violations committed by persons or entities it empowered to exercise elements of governmental authority;

103 For an examination of the technical challenges for attributing cyber attacks to specific actors, see Vitaly Kamluk, "Know Your Enemy and Know Yourself: Attribution in the Cyber Domain", *Humanitarian Law and Policy Blog*, 3 June 2019, available at: https://blogs.icrc.org/law-and-policy/2019/06/03/know-your-enemy-know-yourself-cyber-domain-attribution/.
104 ICRC Challenges Report 2011, above note 43, p. 36.
105 ICRC, above note 1, p. 9.
106 *Ibid.*

(c) violations committed by persons or groups acting in fact on its instructions, or under its direction or control; and
(d) violations committed by private persons or groups which it acknowledges and adopts as its own conduct.[107]

These principles apply whether the violation of IHL has been committed by cyber means or by any other means.[108]

The limits that IHL imposes on the use of cyber capabilities during armed conflicts

Recognizing that IHL applies to cyber operations having a nexus to an armed conflict is only a first step. The specific characteristics of this new technology raise several challenges for the interpretation of IHL rules, including those on the conduct of hostilities.

The partly non-physical (i.e., digital) nature of cyberspace and the interconnectedness of military and civilian networks pose practical and legal challenges in applying the general IHL rules protecting civilians and civilian objects against cyber operations, in particular those amounting to attacks under IHL. It is even suggested that it may be impossible, at times, to apply basic IHL principles in cyberspace. As will be shown below, this challenge might be overstated. Nonetheless, key issues arise with regard to protecting essential civilian cyber infrastructure against military attack. As many of the IHL rules governing the conduct of hostilities apply only to military operations that amount to "attacks" as defined in IHL, this section first examines various issues relating to cyber operations that qualify as attacks, including the salient question of *which* operations qualify as attacks under IHL. Second, it explores obligations of parties to armed conflicts in military operations other than those amounting to "attacks". Third, the section analyzes certain challenges regarding the legal review of cyber capabilities.

Cyber operations that amount to an attack under IHL

IHL sets out essential rules restricting cyber operations that amount to "attacks" as defined in IHL. This section looks at those rules and principles that have been subject to the most intense debates. It examines first whether, from a technological perspective, cyber attacks are capable of being directed at specific

107 See ICRC Customary Law Study, above note 63, Rule 149. See also International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, 2001, in particular Arts 4–11.

108 ICRC, above note 1, p. 9; Tallinn Manual 2.0, above note 13, Rules 15–17. For a different view, see the Chinese submission on the initial pre-draft of the report of the OEWG, which states that with regard to "state responsibility, which, unlike the law of armed conflicts or human rights, has not yet gained international consensus, there is no legal basis at all for any discussion on its application in cyberspace". Comments by China on the initial pre-draft of the OEWG report, available at: www.un.org/disarmament/open-ended-working-group/.

military objectives as required by the principle of distinction. The second part analyzes how the notion of attack under IHL should be interpreted in cyberspace. The third part discusses the closely related debate on whether civilian data must be granted the same protection as civilian "objects" for the purposes of IHL, and the final part addresses the ongoing debate on how IHL rules on the conduct of hostilities apply to objects used simultaneously for civilian and military purposes (often called dual-use objects), which are particularly prevalent in cyberspace.

From a technical perspective, cyber attacks can be directed at specific military objectives

Implementing the principles of distinction and proportionality, and the prohibition against indiscriminate attacks, requires that an attack can be and is directed at a military objective and will not cause excessive incidental harm to civilians or civilian objects. Contrary to the assumption that these principles might become meaningless in cyberspace because of the interconnectivity that characterizes it, careful examination of cyber operations shows that such operations are not inherently indiscriminate. For instance, if a cyber operation is carried out by operators who enter a target and carry out an operation, the operators will know where they are and what they are doing. Similarly, analyses of cyber tools show that they are not necessarily indiscriminate. However, programming malware that discriminates between civilian objects and military objectives, and conducting cyber operations without causing excessive incidental damage, requires sophisticated capabilities and testing.

Those who develop malware or plan cyber attacks can design their tools without self-propagation functions. In that case, malware cannot spread without additional human intervention. Even if self-propagating, attacks over the years have shown that malware can be designed to only attack specific hardware or software. This means that even if malware is programmed to spread widely, it can be designed to only cause damage to a specific target or specific sets of targets. Especially cyber attacks that aim to cause physical damage to industrial control systems may require cyber tools that are designed for that specific target and purpose. In many cases, the need for such custom-made tools would effectively hamper – from a technical perspective – the ability to carry out a cyber attack on a large scale or in an indiscriminate manner. The fact that cyber attacks can technically be targeted precisely does not mean they are necessarily lawful if carried out in a conflict. However, the characteristics seen in a number of cyber operations show that they can be very precisely tailored to create effects on specific targets only, and that such operations are therefore capable of complying with IHL principles and rules.

The fact that some of the known cyber tools were designed to self-propagate and caused harmful effects on widely used civilian computer systems does not support an argument that the interconnectedness of cyberspace makes it challenging, if not impossible, to implement basic IHL rules. On the contrary, during armed conflicts, the use of such cyber tools would be prohibited by

IHL.[109] IHL prohibits attacks that employ means and methods of warfare, including cyber means and methods, that cannot be directed at a specific military objective or may be expected to escape the control of the user,[110] or – while being targeted at a military objective – may be expected to cause incidental civilian damage that is excessive in relation to the concrete and direct military advantage anticipated.[111]

The notion of "attack" under IHL and its application to cyber operations

The question of whether or not an operation amounts to an "attack" as defined in IHL is essential for the application of many of the rules deriving from the principles of distinction, proportionality and precaution, which afford important protection to civilians and civilian objects. Concretely, rules such as the prohibition on *attacks* against civilians and civilian objects,[112] the prohibition on indiscriminate[113] and disproportionate *attacks*,[114] and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects when carrying out an *attack*[115] apply to those operations that qualify as "attacks" as defined in IHL. The question of how widely or narrowly the notion of "attack" is interpreted with regard to cyber operations is therefore essential for the applicability of key rules – and the protection they afford to civilians and civilian infrastructure – to cyber operations.

Article 49 of AP I defines attacks as "acts of violence against the adversary, whether in offence or in defence". It is well established that the notion of violence in this definition can refer to either the means of warfare or their effects, meaning that an operation causing violent effects can be an attack even if the means used to cause those effects are not violent as such.[116] On the basis of this understanding, the Tallinn Manual 2.0 proposes the following definition of a cyber attack: "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[117]

It is widely accepted by States that took a position on the issue, by the ICRC and by experts that at least those cyber operations which cause death, injury or

109 Similarly, the DoD Law of War Manual, above note 87, para. 16.6, concludes: "For example, a destructive computer virus that was programmed to spread and destroy uncontrollably within civilian internet systems would be prohibited as an inherently indiscriminate weapon."

110 Yves Sandoz, Christophe Swinarski and Bruno Zimmerman (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), para. 1963.

111 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 51(4)–(5); ICRC Customary Law Study, above note 63, Rules 11, 14.

112 See AP I, Art. 52; ICRC Customary Law Study, above note 63, Rules 7–10.

113 See AP I, Art. 54(c); ICRC Customary Law Study, above note 63, Rule 11.

114 See AP I, Art. 51(5)(b); ICRC Customary Law Study, above note 63, Rule 14.

115 See AP I, Art. 57(1); ICRC Customary Law Study, above note 63, Rule 15.

116 See C. Droege, above note 83, p. 557; William H. Boothby, *The Law of Targeting*, Oxford University Press, Oxford, 2012, p. 384. As Droege points out, "it is uncontroversial that the use of biological, chemical, or radiological agents would constitute an attack, even though the attack does not involve physical force".

117 Tallinn Manual 2.0, above note 13, Rule 92.

physical damage constitute attacks under IHL.[118] Some States expressly include harm due to the foreseeable indirect (or reverberating) effects of attacks,[119] a view that is also taken by the ICRC.[120] This could be the case, for example, if patients in an intensive care unit are killed as a result of a cyber operation against an electricity network that causes the hospital's electricity supply to be cut off.

Beyond this basic consensus, different views exist on whether a cyber operation that disables an object without physically damaging it amounts to an attack under IHL.[121] There were extensive discussions on this issue in the process of drafting the Tallinn Manual. A majority of the experts held that a cyber operation amounts to an attack if it is expected to interfere with functionality and if restoration of functionality requires replacement of physical components. For some experts, a cyber operation will also amount to an attack if the restoration of functionality requires the reinstallation of the operating system or of particular data.

The ICRC has taken the position that an operation designed to disable a computer or a computer network during an armed conflict constitutes an attack as defined in IHL whether or not the object is disabled through destruction or in any other way.[122]

Two main reasons underpin the ICRC's position. The first one results from an interpretation of the notion of attack in its context.[123] Given that the definition of military objectives in Article 52(2) of AP I refers not only to destruction or capture but also to "neutralization" as a possible result of an attack, the notion of "attack" under Article 49 of AP I should be understood to encompass operations designed to impair the functioning of objects (i.e. neutralize them) without causing physical damage or destruction. Indeed, it has been submitted that the explicit mentioning of neutralization under Article 52(2) would be superfluous otherwise.[124] Second,

118 See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, 2015 (ICRC Challenges Report 2015), pp. 41–42, available at: www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf; Tallinn Manual 2.0, above note 13, Rule 92. For States that have taken a view on how the notion of attack under IHL applies to cyber operations, see, in particular, Australian Department of Foreign Affairs and Trade, above note 94, Annex A; Danish Ministry of Defence, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, 2016 (Danish Military Manual), pp. 290–291, available at: www2.forsvaret.dk/omos/publikationer/Documents/Military%20Manual%20updated%202020.pdf; French Ministry of the Armies, above note 77, p. 13; Norway, *Manual i krigens folkerett*, 2013 (Norwegian Military Manual), para. 9.54, available at: https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/194213/manual_krigens_folkerett.pdf?sequence=1&isAllowed=y; New Zealand Military Manual, above note 85, para 8.10.17; DoD Law of War Manual, above note 87, para. 16.5.1.

119 Danish Military Manual, above note 118, p. 677 (when discussing computer network attacks); New Zealand Military Manual, above note 85, para 8.10.22; Norwegian Military Manual, above note 118, para. 9.54.

120 ICRC, above note 1, p. 7.

121 See, for instance, Tallinn Manual 2.0, above note 13, commentary on Rule 92, paras 10–12.

122 See ICRC Challenges Report 2015, above note 119, pp. 41–42. See also Tallinn Manual 2.0, above note 13, para. 12 of the commentary on Rule 92.

123 Vienna Convention on the Law of Treaties, Art. 31(1).

124 Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", 2004, p. 4, available at: www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf; C. Droege, above note 83, p. 559. For a different view, see Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", *International Law Studies*, Vol. 87, 2011, pp. 95–96; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 198.

an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities, which are to ensure the protection of the civilian population and civilian objects against the effects of hostilities. Indeed, under an overly restrictive understanding, a cyber operation that is directed at making a civilian network (electricity, banking, communications or other network) dysfunctional, or risks causing this incidentally, might not be covered by essential IHL rules protecting the civilian population and objects.[125]

In a similar manner, expert commentators suggest that it is important "to interpret the provision [Article 49 of AP I] taking into account the recent technological developments and to expand the concept of 'violence' to include not only material damage to objects, but also incapacitation of infrastructures without destruction".[126]

Because cyber operations can significantly disrupt essential services without necessarily causing physical damage, this constitutes one of the most critical debates for the protection of civilians against the effects of cyber operations. It is therefore crucial for States to express their views on the issue and to work towards a common understanding. For the moment, opinions vary among the States that have taken public positions.

The definitions of the notion of "attack" adopted in the military manuals of Norway and New Zealand mirror the definition adopted by the Tallinn Manual 2.0. It is, however, unclear whether these manuals were meant to express a position on this debate, because the commentary on Rule 92 of the Tallinn Manual 2.0 notes different views of how "damage" should be understood in the cyber context. Australia has stated that cyber operations qualify as attacks if they rise "to the same threshold as that of a kinetic 'attack under IHL'",[127] but it is unclear whether this was intended as a position in this debate.

A few States focus on physical damage to qualify a cyber operation as an attack. According to one OAS study, Peru has opined that in order for an operation to qualify as an attack, people or objects must be "physically harmed".[128] The Danish Military Manual specifies for the term "attack" that "[a]s far as damage to objects is concerned, the term covers any physical damage. However, the term does not cover temporary inoperability and other neutralization which does not involve physical damage (e.g., a digital 'freeze' of a

125 In the same sense, see also M. N. Schmitt, above note 67, p. 339.

126 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 181. See also Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New *Tallinn Manual*", *Journal of Conflict and Security Law*, Vol. 18, No. 2, 2013, p. 341: "It would, indeed, be less than convincing to insist that the term 'attacks' should be limited to acts directly causing injury or physical destruction, when the same action can, eg lead to disrupt [*sic*] essential supplies for hospitals or other important civilian infrastructure."

127 Australian Department of Foreign Affairs and Trade, above note 94, Annex A.

128 OAS, above note 22, para. 43.

communication control system)."[129] In its 2014 submission to the UN GGE, the United States noted:

> When determining whether a cyber activity constitutes an "attack" for *jus in bello* purposes, States should consider, *inter alia*, whether a cyber activity results in kinetic and irreversible effects on civilians, civilian objects, or civilian cyber infrastructure, or non-kinetic and reversible effects on the same.[130]

Along the same lines, the US Department of Defense (DoD) Law of War Manual provides the example of a "cyber attack that would destroy enemy computer systems", and notes that "[f]actors that would suggest that a cyber operation is not an 'attack' include whether the operation causes only reversible effects or only temporary effects".[131] Unfortunately, these documents do not clarify what they mean by "reversible" or "temporary" effects, or what the difference is – if any – between the two notions.[132] They do not discuss whether – and if so, after how long – an effect may no longer be considered temporary, or how to consider repeated operations that would each cause a temporary – but deliberately accumulating – effect. They do not discuss either whether "reversible" refers solely to operations in which the author may reverse the effects of the attack,[133] or also to operations where the target needs to take action to restore the functionality of the targeted system or otherwise end or reverse the effects of the attack. In this respect, it should be remembered that the possibility of repairing physical damage caused by a military operation (whether cyber or kinetic) is not generally understood as a criterion disqualifying an operation as an attack under IHL.[134] This is the case even if the repair reverses the direct effect of that operation and restores the functionality of the object in question.[135]

France has expressed a clearer and broader understanding of the notion of cyber attack. It considers that

129 Danish Military Manual, above note 118, p. 290. The Manual specifies with regard to computer network attacks and operations that "[t]his means, for instance, that network-based operations must be regarded as attacks under IHL if the consequence is that they cause physical damage". *Ibid.*, p. 291.

130 United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2014–15, p. 5.

131 See also DoD Law of War Manual, above note 87, paras 16.5.1, 16.5.2.

132 Gary Brown and Kurt Sanger, "Cyberspace and the Law of War", *Cyber Defense Review*, 6 November 2015, available at: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136032/cyberspace-and-the-law-of-war/.

133 For example, a distributed denial-of-service (DDoS) attack where the targeted network or system would automatically get back to operating normally when the attacker ends the DDoS attack and where no other indirect effect would have been caused during the time that the network or system was affected.

134 Laurent Gisel, "The Use of Cyber Technology in Warfare: Which Protection Does IHL afford and Is It Sufficient?", in G. Venturini and G. L. Beruto (eds), above note 7.

135 For example, Michael Lewis discusses the practice of conducting bridge attacks longitudinally during the 1991 Gulf War, and, *inter alia*, notes that "damage to the bridge would be nearer midspan and therefore more easily repaired", without claiming that this quality would prevent the operation to qualify as an attack. See Michael Lewis, "The Law of Aerial Bombardment in the 1991 Gulf War", *American Journal of International Law*, Vol. 97, No. 3, 2003, p. 501.

> a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterised where action by the adversary is necessary to restore the infrastructure or system (repair of equipment, replacement of a part, reinstallation of a network, etc.).[136]

Commenting this position, Schmitt has noted that "[t]his view is highly defensible as a matter of law, for the plain meaning of damage reasonably extends to systems that do not operate as intended and require some form of repair to regain functionality".[137] In a similar manner, according to the OAS study mentioned above, Chile suggests that for an operation to qualify as an attack, its result must require the affected State to "take action to repair or restore the affected infrastructure or computer systems, since in those cases the consequences of the attack are similar to those described above, in particular physical damage to property".[138] The study also indicated that Guatemala expressed the position that a cyber operation which "only produce[s] a loss of functionality" would amount to an attack, a position also held by Ecuador.[139] Bolivia, Ecuador and Guyana further specify that such cyber operations may constitute an attack under IHL in particular when they disable critical infrastructure or the provision of basic services to the population.[140]

In any case, not all cyber operations during armed conflicts would constitute "attacks" as understood in IHL. First, the concept of attack in IHL does not include espionage. Second, the rules on the conduct of hostilities do not prohibit all operations that interfere with civilian communication systems: the jamming of radio communications or television broadcasts has traditionally not been considered an attack as defined in IHL. However, the distinction between attacks and interferences with communications that do not amount to an attack is probably less clear in cyber operations than in more traditional kinetic or electromagnetic operations.[141] Third, the notion of "military operations" under IHL, including those carried out by cyber means, is broader than the notion of "attacks", as will be discussed below.

136 French Ministry of the Armies, above note 77, p. 13.
137 M. N. Schmitt, above note 52. In the same sense, see W. H. Boothby, above note 116, p. 386.
138 OAS, above note 22, para. 43.
139 Ecuador specified that "[a] cyber operation can qualify as an attack if it renders inoperable a state's critical infrastructure or others that endanger the security of the state". *Ibid.*, para. 44.
140 Bolivia suggested that a cyber operation "could be considered an attack when its objective is to disable a state's basic services (water, electricity, telecommunications, or the financial system"); Guyana suggested that "cyber operations that undermine the functioning of computer systems and infrastructure needed for the provision of services and resources to the civilian population constitute an attack", among which it included "nuclear plants, hospitals, banks, and air traffic control systems". *Ibid.*, paras 44–45.
141 ICRC Challenges Report 2015, above note 118, pp. 41–42; C. Droege, above note 83, p. 560.

The protection of data as a "civilian object"

In addition to the foundational question of which cyber operations amount to "attacks" under IHL, the question of whether civilian data enjoys the same protection as civilian objects has been subject to significant debate and remains unsettled. The protection of civilian data against malicious cyber operations during armed conflict is becoming increasingly important because data is an essential component of the digital domain and a cornerstone of life in many societies: individual medical data, social security data, tax records, bank accounts, companies' client files, and election lists and records are key to the functioning of most aspects of civilian life. As this trend is expected to continue, if not accelerate, in years to come, there is increasing concern about safeguarding such essential civilian data.

With regard to data belonging to certain categories of objects that enjoy specific protection under IHL, the protective rules are comprehensive. As discussed below, the obligations to respect and protect medical facilities and humanitarian relief operations must be understood as extending to medical data belonging to those facilities and data of humanitarian organizations that are essential for their operations.[142] Similarly, deleting or otherwise tampering with data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation systems, is prohibited.[143]

Still, it is important to clarify the extent to which civilian data are protected by the existing general rules on the conduct of hostilities. In particular, debate has arisen on whether data constitute objects as understood under IHL, in which case cyber operations against data (such as deleting them) would be governed by the principles of distinction, proportionality and precaution and the protection they afford to civilian objects.[144]

This question is closely related to discussions on the notion of "attack" above. To start with, 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. This is the case because the consequences of an operation against data can qualify that operation as an attack under IHL and therefore subject to pertinent IHL. For these attacks, it is not important whether or not data qualifies as an object under IHL.

142 See discussion in the above section entitled "IHL Rules Protecting Objects Indispensable to the Survival of the Civilian Population".

143 AP I, Art. 54; Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II), Art. 14; ICRC Customary Law Study, above note 63, Rule 54.

144 See Tallinn Manual 2.0, above note 13, paras 6–7 of the commentary on Rule 100. For academic discussion, see *Israel Law Review*, Vol. 48, No. 1, pp. 39–132; M. N. Schmitt, above note 67.

The question of whether data are objects for the purpose of IHL is, however, critical for operations that are not designed or expected to cause such consequences. Broadly speaking, two general approaches can be considered. Under the first approach, which considers data as objects under IHL, an operation designed or expected to delete or manipulate data would be an attack governed by all the relevant IHL rules because it would amount to destroying or damaging an object (the data). This would also be the case if such deletion or manipulation were not expected to cause death or injury to a person or to damage or disable a physical object. Even under this view, however, an operation designed solely to access (possibly confidential) data without deleting or manipulating them – such as spying – would not be an attack.

Conversely, if data are not considered to be objects under IHL, an operation designed to delete or manipulate them without causing death or injury to a person or damage to an object would not be governed by the rules on attacks, or by some of the more general rules affording protection to civilian objects (such as the obligation to take constant care to spare civilians and civilian objects, as discussed below in the section on "Rules Governing Military Operations Other than Attacks"). The operations could, however, be governed by other specific protection regimes under IHL, which will be analyzed below in the section on "IHL Rules Protecting Objects Indispensable to the Survival of the Civilian Population, Medical Services, and Humanitarian Relief Operations". Still, there would be a gap in protection for essential civilian data that do not benefit from a specific protection regime, and this would raise concern.

Experts hold different views on whether data qualify as objects for the purposes of the IHL rules on the conduct of hostilities.[145] One view, held by the majority of experts involved in the Tallinn Manual process, is that the ordinary meaning of the term "object", as discussed in the 1987 ICRC Commentary on AP I, cannot be interpreted as including data because objects are material, visible and tangible.[146] The relevant explanation in the ICRC Commentary, however, aims at distinguishing objects from concepts such as "aim" or "purpose", not at differentiating between tangible and intangible goods, and therefore cannot be seen as determinative for the debate on data.[147] In contrast, others have argued that either all or some types of data should be considered as objects under IHL. One view is that the "modern meaning" of the notion of objects in today's society, and an

145 For an illustration of this debate, see "Scenario 12: Cyber Operations against Computer Data", in K. Mačák, T. Minárik and T. Jančárková (eds), above note 68.

146 The Oxford Dictionary defines an object as "a material thing that can be seen and touched". Recalling the ordinary meaning of the word object, the 1987 ICRC Commentary on the Additional Protocols describes an object as "something that is visible and tangible". ICRC Commentary on the APs, above note 110, para. 2008. See also Tallinn Manual 2.0, above note 13, para. 6 of the commentary on Rule 100. It is interesting to note here that today, the Oxford Dictionary includes a specific definition of objects for computing: "A data construct that provides a description of anything known to a computer (such as a processor or a piece of code) and defines its method of operation."

147 See also International Law Association (ILA) Study Group on the Conduct of Hostilities in the 21st Century, "The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare", *International Law Studies*, Vol. 93, 2017 (ILA Report), pp. 338–339.

interpretation of the term in light of its object and purpose, must lead to the conclusion that "data is an 'object' for the purposes of the IHL rules on targeting".[148] This interpretation is supported by the traditional understanding of the notion of "object" under IHL, which is broader than the ordinary meaning of the word and encompasses also locations and animals. Another proposal is to differentiate between "operational-level data", or "code", and "content-level data".[149] In this model, it has been argued that, notably, operational-level data may qualify as a military objective, which implies that this type of data could also qualify as a civilian object.[150] While considering operational data as objects would align with the view discussed above that disabling objects constitutes an attack, it does not appear to provide additional protection. In this debate, it has been argued that none of the proposed conclusions is entirely satisfactory, each being either under- or over-inclusive.[151]

For its part, the ICRC has stressed the need to safeguard essential civilian data, emphasizing that in cyberspace, deleting or tampering with data could quickly bring government services and private businesses to a complete standstill and could thereby cause more harm to civilians than the destruction of physical objects. Thus, in the ICRC's view the conclusion that this type of operation would not be prohibited by IHL in today's ever more cyber-reliant world seems difficult to reconcile with the object and purpose of this body of norms.[152] Logically, the replacement of paper files and documents with digital data should not decrease the protection that IHL affords to them.[153] As the ICRC has emphasized, "[e]xcluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap".[154]

So far, few States have expressed views on whether the notion of "object" should be understood to encompass data for the rules governing the conduct of hostilities. For example, the Danish Military Manual considers that "(digital) data do not in general constitute an object".[155] Conversely, the Norwegian Military

148 Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law", *Israel Law Review*, Vol. 48, No. 1, 2015, p. 80; Robert McLaughlin, "Data as a Military Objective", Australian Institute of International Affairs, 20 September 2018, available at: www.internationalaffairs.org.au/australianoutlook/data-as-a-military-objective/.

149 Under the proposed distinction, content-level data would include data "such as the text of this article, or the contents of medical databases, library catalogues and the like", whereas operational-level data would describe "essentially the 'soul of the machine'", meaning the "type of data that gives hardware its functionality and ability to perform the tasks we require". Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review*, Vol. 48, No. 1, 2015, p. 41.

150 *Ibid.*, p. 54.

151 Schmitt therefore argues that as a matter of policy, States should "accord special protection to certain 'essential civilian functions or services' by committing to refrain from conducting cyber operations against civilian infrastructure or data that interfere with them". M. N. Schmitt, above note 67, p. 342.

152 ICRC Challenges Report 2015, above note 118, p. 43.

153 ICRC Challenges Report 2019, above note 36, p. 21.

154 ICRC, above note 1, p. 8. See also P. Pascucci, above note 67, who notes that the position adopted by the majority of the experts in the Tallinn Manual with regard to data creates a "seemingly expansive gap in what constitutes an object", and later argues that "[i]t is unrealistic in an information age for data to fall outside the scope of constituting an object, thus failing to receive IHL protection associated with the principles of distinction and proportionality".

155 Danish Military Manual, above note 118, p. 292.

Manual holds that data shall be regarded as objects and may only be attacked directly if they qualify as a lawful target.[156] France has expressed what could be seen as a middle-ground view, stating that "[g]iven the current state of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction".[157] The description of Peru's position in the OAS's *Improving Transparency* report appears to reflect a similar position: while not expressly taking a position on whether data are objects, Peru's position is explained as assessing operations against data under the notion of "military objective", suggesting that some data systems may not be subjected to attacks because such attacks would "not create a legitimate military advantage".[158] As the definition of "military objectives" under Article 52(2) of AP I applies "in so far as objects are concerned", this reasoning appears to imply that data constitute objects. Chile proposes to look at the effects of an attack against data, concluding that "[t]he principle of distinction must therefore be taken into consideration in the context of cyber operations, whereby a state should refrain from attacking data in case it could affect the civilian population". Reportedly, Chile has further emphasized that "an attack directed exclusively at computer data could well produce adverse consequences affecting the civilian population".[159]

In an increasingly data-reliant world, the question of how States interpret and apply IHL rules to safeguard essential data against destruction, deletion or manipulation will be a litmus test for the adequacy of existing humanitarian law rules.

The protection of cyber infrastructure serving simultaneously military and civilian purposes

In order to protect critical civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of cyberspace itself. The challenge lies, however, in the interconnectedness of civilian and military networks. Most military networks rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Civilian vehicles, shipping and air traffic control are increasingly equipped with navigation equipment that relies on global navigation satellite system (GNSS) satellites such as BeiDou, GLONASS, GPS and Galileo, which may also be used by the military. Civilian logistical supply chains (for food and medical supplies) and other businesses use the same web and communication networks through which some military communication passes. Except for certain networks that are specifically dedicated to military use, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures.

156 Norwegian Military Manual, above note 118, para. 9.58.
157 French Ministry of the Armies, above note 77, p. 14.
158 OAS, above note 22, para. 49, fn. 115.
159 *Ibid.*, para. 48.

Under IHL, attacks must be strictly limited to military objectives. Insofar 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 total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. All objects which are not military objectives under this definition are civilian objects under IHL and must not be made the object of an attack or of reprisals. In case of doubt as to whether an object that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed to remain protected as a civilian object.[160]

It is traditionally understood that an object may become a military objective when its use for military purposes is such that it fulfils the definition of military objective even if it is simultaneously used for civilian purposes. A wide interpretation of this rule could lead to the conclusion that many objects forming part of cyberspace infrastructure would constitute military objectives and would therefore not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ever-increasing civilian reliance on cyberspace.

Such a conclusion would, however, be incomplete. First, the analysis of when a civilian object becomes a military objective cannot be done for cyberspace or the Internet in general. Instead, belligerents must identify which computer, nodes, routers or networks might have become a military objective. In this respect, parts of the network, specific computers, or other hardware that can be separated from a network or system as a whole need to be analyzed individually. The means and methods used must enable directing the attack at the specific military objective(s) that may have been identified, and all feasible precautions must be taken to avoid or at least minimize incidentally affecting the remaining civilian objects or parts of the network.[161] It has also been argued that it is prohibited to treat as a single target a number of clearly discrete cyber military objectives in cyber infrastructure primarily used for civilian purposes if to do so would harm protected persons or objects.[162] Second, cyberspace is designed with a high level of redundancy, meaning that one of its characteristics is the ability to immediately re-route data traffic. This inbuilt resilience needs to be considered when assessing whether the target's destruction or neutralization would offer a definite military advantage as required by the definition of a military objective. If this is not the case, the object would remain civilian and cannot be attacked. And third, any attack is governed by the prohibition against indiscriminate attacks and the rules of proportionality and precautions in attack. Stopping or impairing the civilian use of an object in violation of one of these rules would

160 See AP I, Art. 52. ICRC Customary Law Study, above note 63, Rules 7–10.
161 See AP I, Arts 51(4), 57(2)(a)(ii); ICRC Customary Law Study, above note 63, Rules 12–17.
162 See Tallinn Manual 2.0, above note 13, Rule 112, which derives from the prohibition on area bombardment found in Article 51(5)(a) of AP I and customary IHL (see ICRC Customary Law Study, above note 63, Rule 13).

render the attack unlawful despite the fact that the object had become a military objective.[163]

Compared to kinetic military operations, the use of cyber operations may, depending on the circumstances, enable achieving a particular effect while causing less destruction (on the target or incidentally on other objects or systems) or causing damage that may be more easily repaired or restored. This consideration is particularly relevant with regard to dual-use objects, as illustrated by the scenario of a belligerent trying to neutralize an enemy underground command bunker by cutting its electricity supply, which is simultaneously providing power to civilian infrastructure. A cyber operation may allow the operator to remotely choose which parts of the network to switch off.[164] This could enable the attacker to achieve the desired effect while avoiding, or at least minimizing, harmful effects to the delivery of electricity to civilians. In such a case, and provided that choosing to use a cyber operation instead of a kinetic one is *feasible*, conducting the cyber operation would become required by the principle of precaution. Indeed, the obligation to take all feasible precautions in the choice of means and methods of warfare to avoid or at least minimize incidental civilian harm[165] is technologically neutral: it also applies to means and methods relying on new technologies, and may even require their use.[166] Whether this is feasible in a specific instance depends on the circumstances ruling at the time, including humanitarian and military considerations.[167]

Limitations on cyber operations other than those amounting to "attacks", including the specific protection of certain persons and objects

While many of the general rules on the conduct of hostilities are limited to acts amounting to attacks as defined in IHL, some IHL rules governing the conduct of hostilities apply to a broader set of operations: first, a few rules apply to all "military operations", and second, the specific protection afforded to certain categories of persons and objects goes beyond the protection against attacks.

163 While acknowledging that the other view also exists, the ILA Study Group on the Conduct of hostilities deemed this "the better view" based on State practice, official documents and doctrine: see ILA Report, above note 147, pp. 336–337. See also ICRC, *International Expert Meeting Report: The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, Geneva, 2018, p. 39, available at www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality; Helen Durham, Keynote Address, in Edoardo Greppi (ed.), *Conduct of Hostilities: The Practice, the Law and the Future*, 37th Round Table on Current Issues of International Humanitarian Law, International Institute of Humanitarian Law, Sanremo, 2015, p. 31.

164 This was reportedly done in the 2015 cyber operations against the electricity grid in Ukraine. See Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", *Wired*, 3 March 2016, available at: www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

165 AP I, Art. 57(2)(a)(ii); ICRC Customary Law Study, above note 63, Rule 17.

166 See ILA Report, above note 147, p. 384.

167 While military considerations might include the "fragility" of cyber means and methods, this is not the only relevant factor determining feasibility. It is not possible to rule out that it is feasible, and therefore required, to use cyber operations to avoid or minimize incidental civilian harm on the sole basis that the cyber means or methods used are "fragile", without looking at the entirety of the situation, including all relevant humanitarian considerations.

Rules governing military operations other than attacks

Identifying, and possibly clarifying, the rules that offer general protection to the civilian population and civilian objects against the effects of cyber operations that do not amount to attacks is an issue requiring more attention. This is all the more critical if the view is taken that only those operations causing physical damage are considered as attacks: in that case, there would be a rather broad category of cyber operations to which only a limited set of IHL rules applies. Such a conclusion would cause real concern for the protection of civilians and civilian infrastructure.

The notion of "military operation" appears in a number of articles of the 1949 Geneva Conventions and their 1977 Additional Protocols.[168] Of most interest here are the rules that regulate the conduct of military operations, including those carried out by cyber means. They include the basic rule that "parties to the conflict … shall direct their operations only against military objectives" (AP I, Article 48), the principle that "the civilian population and individual civilians shall enjoy general protection against dangers arising from military operations" (AP I, Article 51(1)),[169] and the obligation that "constant care shall be taken to spare the civilian population, civilians and civilian objects" in the conduct of military operations (AP I, Article 57(1)).[170]

The ordinary meaning of the term "military operation" and a systematic interpretation of these articles lead to the conclusion that this notion is different from the notion of "attack" as defined in Article 49 of AP I.[171] While the ICRC Commentary on Article 48 of AP I notes that the notion refers to military operations during which violence is used, and not to ideological, political or religious campaigns, it clarifies that it is a broader notion than "attacks". The Commentary defines "military operations" for the purpose of these articles as "any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat" or "related to hostilities" – an understanding that is widely accepted.[172]

168 See GC III, Art. 23; GC IV, Art. 28; AP I, Arts 3, 39, 44, 51, 56–60; AP II, Art. 13.

169 See also AP I, Art. 58; AP II, Art. 13(1).

170 See also ICRC Customary Law Study, above note 63, Rule 15; Tallinn Manual 2.0, above note 13, Rule 114.

171 An interpretation that assimilates the notions of "operation" and "attack" would deprive the rules applying to "operations" of meaningful content and render them essentially superfluous. See C. Droege, above note 83, p. 556.

172 ICRC Commentary on the APs, above note 110, paras 2191, 1936, 1875. In the same vein, see Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflict: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Leiden, 2013, para. 2.2.3 on Art. 48, para. 2.8.2 on Art. 57; UK Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, Joint Service Publication 383, 2004 (UK Military Manual), para 5.32, fn. 187; ILA Report, above note 147, p. 380. The *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Program on Humanitarian Policy and Conflict Research, Harvard University, 2009) applies the constant care obligation to "air or missile combat operations" (Rule 34), a notion broader than "attack" that includes, *inter alia*, refuelling, jamming of enemy radars, use of airborne warning systems and dropping an airborne force (commentary on Rule 1(c), para. 3). See also Noam Neuman, "A Precautionary Tale: The Theory and Practice of Precautions in Attack", *Israel Yearbook on Human Rights*, Vol. 48, 2018, p. 28; Jean-François Quéguiner, "Precautions under

The notion is mostly discussed in relation to the treaty and customary obligation to take constant care to spare the civilian population, civilians and civilian objects in the conduct of military operations. France has explicitly stated that this obligation also applies in cyberspace.[173] This obligation requires all those involved in military operations to continuously bear in mind the effects of military operations on the civilian population, civilians and civilian objects, to take steps to reduce such effects as much as possible, and to seek to avoid any unnecessary effects.[174] It has been described as a positive and continuous obligation aimed at risk mitigation and harm prevention that imposes requirements which increase commensurably with the risk to civilians.[175] The Tallinn Manual explains in this respect that

> [t]he law admits of no situation in which, or time when, individuals involved in the planning and execution process may ignore the effects of their operations on civilians or civilian objects. In the cyber context, this requires situational awareness at all times, not merely during the preparatory stage of an operation.[176]

A more challenging issue is the application of the principle of distinction to military operations other than attacks. As noted above, Article 48 of AP I requires that military operations be directed only against military objectives. While the commentaries by the ICRC and by Bothe, Partsch and Solf[177] underline the fundamental character of this article, they do not shed much light on the precise meaning and scope of this obligation, which remain subject to debate.

Article 48 is sometimes understood as an overarching principle that is implemented through the application of the various rules of the section of the Protocol that it opens. Some commentators therefore argue that the specific rules stemming from the principle of distinction apply only to attacks and not to military operations other than attacks.[178] Accordingly, some military manuals

the Law Governing the Conduct of Hostilities", *International Review of the Red Cross*, Vol. 88, No. 864, 2006, p. 797; Chris Jenks and Rain Liivoja, "Machine Autonomy and the Constant Care Obligation", *Humanitarian Law and Policy*, 11 December 2018, available at: https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/. Specifically with regard to cyber operations, see Tallinn Manual 2.0, above note 13, para. 2 of the commentary on Rule 114 (noting that the notion of hostilities, to which it applies the constant care obligation, is broader than the notion of attacks); H. Harrison Dinniss, above note 124, p. 199. For a different view at least with regard to the principle of distinction, see M. Roscini, above note 127, p. 178.

173 French Ministry of the Armies, above note 77, p. 15.

174 UK Military Manual, above note 172, para. 5.32.1; Tallinn Manual 2.0, above note 13, para. 4 of the commentary on Rule 114; Dieter Fleck, *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 199; N. Neuman, above note 172, pp. 28–29.

175 ILA Report, above note 147, p. 381.

176 Tallinn Manual 2.0, above note 13, para. 4 of the commentary on Rule 114.

177 M. Bothe, K. J. Partsch and W. A. Solf, above note 172.

178 M. Roscini, above note 126, p. 178. See also, though expressed under customary law, Tallinn Manual 2.0, above note 13, para. 5 of the commentary on Rule 93; Michael N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context", in Christian Czosseck, Rain Ottis and Katharina Ziolkowski (eds), *4th International Conference on Cyber Conflict: Proceedings*, NATO CCD COE Publications, Tallinn, 2012, pp. 283–293, 289–290.

expressly state that cyber operations other than attacks may be directed at civilians or civilian objects.[179] This assertion would seem difficult to reconcile with Article 48 for States party to the Protocol, or at least would need to be carefully articulated. Indeed, experts have pointed out that "[w]hile … there is a distinction between military operations and attacks, it does not follow that non-violent computer network attacks may be therefore conducted against civilian objects".[180] This conclusion stems from the rules of treaty interpretation, which require that provisions are interpreted to "have a meaningful content and are not superfluous".[181]

As noted above, "military operations" are understood as any movements, manoeuvres or other activities whatsoever carried out by the armed forces with a view to combat or related to hostilities. Manoeuvring is also an integral part of cyber operations.[182] For instance, establishing remote access to one system or device might be a step towards reaching or attacking another system or device.[183] Assuming that the former system or device is civilian in character and the latter is a military objective, the question may arise as to whether establishing access to the civilian system or device would be a prohibited military operation. In the view of the present authors, provided that the civilian system or device is not damaged or disabled in the process, such a scenario does not appear to contravene Article 48 because the operation is, ultimately, directed at a military objective.[184] Such cyber operations may indeed be assessed in the same way as traditional military operations – for example, when a commando moves through a civilian house to attack a military objective which is located behind it. Still, other obligations would remain relevant, such as the obligation to take constant care to spare civilian objects.

In the view of the present authors, Article 48, alone or in combination with Articles 51(1) and 57(1) of AP I, should be interpreted as prohibiting cyber operations designed solely at disrupting internet services for the civilian population even if such cyber operations do not disable objects or otherwise have consequences that qualify them as attacks. The civilian use of the Internet is today so all-pervading that any other interpretation would leave an important gap in the protection that IHL affords to civilians against the effects of hostilities carried out by cyber means.[185]

179 Norwegian Military Manual, above note 118, para. 9.57. See also DoD Law of War Manual, above note 87, para. 16.5.2.

180 H. Harrison Dinniss, above note 124, p. 199.

181 See also C. Droege, above note 83, p. 556.

182 See, for example, US DoD, *Cyberspace Operations*, Joint Publication 3-12, 8 June 2018, p. xii: "Movement and Maneuver. Cyberspace operations enable force projection without the need to establish a physical presence in foreign territory. Maneuver in the DODIN [Department of Defense Information Network] or other blue [friendly] cyberspace includes positioning of forces, sensors, and defenses to best secure areas of cyberspace or engage in defensive actions as required. Maneuver in gray [neutral] and red [enemy] cyberspace is a cyberspace exploitation action and includes such activities as gaining access to adversary, enemy, or intermediary links and nodes and shaping this cyberspace to support future actions."

183 L. Gisel and L. Olejnik (eds), above note 11, p. 57.

184 Compare with H. Harrison Dinniss, above note 124, p. 201.

185 The experts who drafted the Tallinn Manual discussed whether disrupting all email communications throughout a country during an armed conflict would amount to an attack – a narrower notion than

As discussed above, some hold the view that not all cyber operations which disable objects, or which delete or manipulate data, constitute attacks. As a consequence of such interpretations, a significantly broader range of cyber operations would not be governed by the rules on attacks, including operations that would create a significant risk of harm. It is therefore all the more important for the protection of the civilian population that those who interpret narrowly the notions of "attack" and "objects" clarify whether they consider that cyber operations which merely disable objects or delete data amount to "military operations", and what this means for the application of the principle of distinction to such operations – in particular, what the requirement of Article 48 of AP I that parties to armed conflicts "shall direct their operations only against military objectives" entails. For instance, at least a certain level of protection would be retained if those who interpret the notion of "attack" narrowly accept that a cyber operation that merely disables objects is a "military operation" which as a consequence must be directed only against military objectives.

Even cyber operations that do not fall within the notion of "military operation" as understood in AP I might be regulated by some IHL rules stemming from the principle of distinction. For example, it has been noted that "directing" psychological operations or other types of propaganda at civilians would not violate Article 48 of AP I because these operations would not fall within the meaning of "military operations" as understood in Article 48.[186] Yet, psychological operations are not beyond the protective reach of other IHL norms. For instance, they must not amount to prohibited acts or threats of violence the primary purpose of which is to spread terror among the civilian population or encourage IHL violations.[187]

Limitations on cyber operations other than attacks may also stem from the principle of military necessity. Relying on the customary rule going back to the 1907 Hague Regulation, the US DoD Law of War Manual states that "[a] cyber operation that would not constitute an attack, but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war".[188] The Manual also refers to military necessity in a more generic manner, specifying that cyber operations which do not amount to attack "must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary".[189] In a similar manner, Australia notes that "[a]pplicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity".[190] While these references to military necessity as a restraining principle are

military operations. While a minority held the view that the international community would generally regard such an operation as an attack, the majority held the view that IHL did not presently extend this far, but nevertheless considered that there was logic in characterizing these operations as attacks. Tallinn Manual 2.0, above note 13, para. 13 of the commentary on Rule 92.

186 C. Droege, above note 83, p. 556.

187 ICRC Challenges Report 2019, above note 36, pp. 28–29.

188 DoD Law of War Manual, above note 87, para. 16.5.1.

189 *Ibid.*, para. 16.5.2.

190 Australian Department of Foreign Affairs and Trade, above note 94, p. 4.

welcome, more clarity is needed on exactly what the principle of military necessity prescribes when conducting cyber operations.

This brief discussion shows that cyber operations other than attacks are not unregulated. The legal regime governing military operations remains, however, less complete, precise and demanding than the legal regime governing operations that amount to attacks under IHL. To address this protection gap at least to some extent, Schmitt has put forward a suggestion that States should apply – as a matter of policy – an adapted proportionality assessment to cyber operations that do not amount to attacks.[191]

The specific protection that IHL provides to certain persons and objects further restricts the scope of permissible military operations.

IHL rules protecting objects indispensable to the survival of the civilian population, medical services, and humanitarian relief operations

In addition to the general rules on the conduct of hostilities, IHL sets out specific regimes for certain objects and services that afford additional and stronger protection than the protection granted to all civilians and civilian objects.

For instance, IHL specifically makes it illegal "to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population".[192] This rule protects, for example, "food-stuffs", "agricultural areas for the production of food-stuffs", and "drinking water installations and supplies and irrigation works".[193] While the experts who drafted the Tallinn Manual held that the Internet as such cannot be considered as an object indispensable to the survival of the civilian population, they noted that "cyber infrastructure indispensable to the functioning of electrical generators, irrigation works and installations, drinking water installations, and food production facilities could, depending on the circumstances, qualify".[194] The explicit mention of "rendering useless" must be understood as covering a broader range of operations that may impact these goods, beyond attacks or destruction. As noted in the ICRC Commentary on Article 54(2) of AP I, the intent of the drafters was "to cover all possibilities" of how objects for the subsistence of the civilian population can be rendered useless.[195] Today, cyber operations that are designed, or can be expected, to render objects indispensable for the civilian population useless are prohibited, regardless of whether they amount to an attack. The debate on whether military operations against these objects amount to an attack (as discussed above) is therefore moot for these objects.

191 M. N. Schmitt, above note 67, p. 347: "States would commit, as a matter of policy, to refraining from conducting cyber operations to which the IHL rules governing attacks do not apply when the expected concrete negative effects on individual civilians or the civilian population are excessive relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation."
192 See AP I, Art. 54(2); AP II, Art. 14; ICRC Customary Law Study, above note 63, Rule 54.
193 AP I, Art. 54(2).
194 Tallinn Manual 2.0, above note 13, para. 5 of the commentary on Rule 141.
195 ICRC Commentary on the APs, above note 110, paras 2101, 2103.

IHL also provides specific protection for medical services. Given the fundamental importance of health care for anyone affected by armed conflict, belligerents must respect and protect medical facilities and personnel at all times.[196] The obligation to "respect" medical facilities and personnel is understood as not only protecting them against operations that amount to attacks – it is prohibited to "harm them in any way. This also means that there should be no interference with their work (for example, by preventing supplies from getting through) or preventing the possibility of continuing to give treatment to the wounded and sick who are in their care."[197] The special protection of medical facilities includes medical communication: while jamming enemy communication is generally considered permissible, "an intentional disruption of [medical] units' ability to communicate for medical purposes" may not be permissible, even if medical units communicate with the armed forces.[198] Moreover, the obligation to respect and protect medical facilities encompasses a prohibition against deleting, altering or otherwise negatively affecting medical data.[199] It may also provide protection against cyber operations directed at the confidentiality of medical data, which at least in some circumstances would be hard to reconcile with the obligation to protect and respect medical facilities.[200] Relevant data in the medical context include "data necessary for the proper use of medical equipment and for tracking the inventory of medical supplies" as well as

196 See, for instance, GC I, Art. 19; GC II, Art. 12; GC IV, Art. 18; AP I, Art. 12; AP II, Art. 11; ICRC Customary Law Study, above note 63, Rules 25, 28, 29; Tallinn Manual 2.0, above note 13, Rules 131–132. Protection of medical facilities and personnel ceases only if they commit, or are used to commit, outside their humanitarian duties, acts harmful to the enemy. Protection may, however, cease only after a due warning has been given, naming, in all appropriate cases, a reasonable time limit, and after such warning has remained unheeded. See GC I, Art. 21; GC II, Art. 34; GC IV, Art. 19; AP I, Art. 13; AP II, Art. 11(2); ICRC Customary Law Study, above note 63, Rules 25, 28, 29; Tallinn Manual 2.0, above note 13, Rule 134.

197 ICRC Commentary on the APs, above note 110, para. 517. See also ICRC Commentary on GC I, above note 69, para. 1799; Oxford Statement, above note 32, point 5 ("During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations"); Tallinn Manual 2.0, above note 13, para. 5 of the commentary on Rule 131 ("For instance, this Rule [Rule 131, which states that "[m]edical and religious personnel, medical units, and medical transports must be respected and protected and, in particular, may not be made the object of cyber attack"] would prohibit altering data in the Global Positioning System of a medical helicopter in order to misdirect it, even though the operation would not qualify as an attack on a medical transport").

198 ICRC Commentary on the APs, above note 110, para. 1804.

199 See ICRC Challenges Report 2015, above note 118, p. 43.

200 See L. Gisel and L. Olejnik (eds), above note 11, p. 36, discussing the hypothetical of hacking into the medical or administrative records of a medical facility in order to gain knowledge of an enemy commander's medical appointment so as to locate him in order to capture or kill him on the way to or back from the medical facility. This could indeed unduly impede the facility's medical functioning and hinder the ability of health-care professionals to uphold their ethical duty of preserving medical confidentiality. The Tallinn Manual 2.0, above note 13, para. 2 of the commentary on Rule 132, proposes the following as an example of an operation that would not violate IHL: "non-damaging cyber reconnaissance to determine whether the medical facility or transports (or associated computers, computer networks, and data) in question are being misused for militarily harmful acts".

"personal medical data required for the treatment of patients".[201] The obligation to "protect" medical facilities, including their data, entails positive obligations. Parties to the conflict must actively take measures to protect medical facilities from harm to the extent feasible, including harm resulting from cyber operations.[202]

IHL also prescribes that humanitarian personnel and relief consignments must be respected and protected.[203] This obligation certainly prohibits any "attacks" against humanitarian operations. In the same way as for the obligation to respect and protect medical personnel and facilities, relevant rules should also be understood as prohibiting "other forms of harmful conduct outside the conduct of hostilities" against humanitarians or undue interference with their work.[204] Moreover, parties to armed conflicts are required to agree, allow and facilitate humanitarian relief operations.[205] Accordingly, Rule 145 of the Tallinn Manual 2.0 states that "cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance", and specifies that such operations are prohibited "even if they do not rise to the level of an 'attack'".[206] The obligation to respect and to protect relief personnel and operations should also be understood as protecting relevant data.[207] At least for States party to AP I, the protection of humanitarian data should encompass data of the ICRC that the organization needs "to carry out the humanitarian functions assigned to it by the [Geneva] Conventions and this Protocol in order to ensure protection and assistance to the victims of conflicts".[208]

These special protections show that IHL provides more stringent rules for military operations against certain goods or services that are essential for the survival, health and well-being of the civilian population.

The importance of legal reviews of cyber means and methods of warfare to ensure respect for IHL

In light of the particular challenges that the characteristics of cyberspace pose to the interpretation and application of some IHL principles in the conduct of hostilities, parties to armed conflicts who choose to develop, acquire or adopt weapons, means or methods of warfare relying on cyber technology need to exercise care in doing so. In this respect, States party to AP I that develop or acquire cyber warfare

201 Tallinn Manual 2.0, above note 13, para. 3 of the commentary on Rule 132.
202 ICRC Commentary on GC I, above note 69, paras 1805–1808; Tallinn Manual 2.0, above note 13, para. 6 of the commentary on Rule 131.
203 AP I, Arts 70(4), 71(2); ICRC Customary Law Study, above note 63, Rules 31, 32.
204 ICRC Commentary on GC I, above note 69, paras 1358, 1799.
205 See, for instance, GC IV, Art. 59; AP I, Arts 69–70; ICRC Customary Law Study, above note 63, Rule 55.
206 Tallinn Manual 2.0, above note 13, para. 4 of the commentary on Rule 80.
207 For further discussion, see Tilman Rodenhäuser, "Hacking Humanitarians? IHL and the Protection of Humanitarian Organizations against Cyber Operations", *EJIL: Talk!*, 16 March 2020, available at: www.ejiltalk.org/hacking-humanitarians-ihl-and-the-protection-of-humanitarian-organizations-against-cyber-operations/.
208 AP I, Art. 81. Such data include, for example, those needed to establish tracing agencies to collect information on persons reported missing in the context of an armed conflict, or those collected by the ICRC when visiting and interviewing detainees without witnesses.

capacities – whether for offensive or defensive purposes – have an obligation to assess whether the employment of the cyber weapon, means or method of warfare would be prohibited by international law in some or all circumstances.[209] More broadly, legal reviews are critical for all States to ensure respect for IHL by their armed forces,[210] so that they only use weapons, means or methods of warfare, including those relying on cyber technology, that comply with the State's obligations under IHL.[211] Such reviews should involve a multi-disciplinary team including legal, military and technical experts as relevant.[212] These legal reviews need to be conducted earlier and in more depth than the analysis of the legality of the actual use of a tool in the specific circumstance of an attack.

In view of the novelty of the technology, it is critical that the legal review of cyber weapons, means and methods of warfare is given particular attention. The prohibition of weapons that are by nature indiscriminate may be particularly relevant considering the ability of certain cyber tools to self-propagate autonomously.[213] The legal review of cyber weapons, means and methods of warfare may, however, present a number of challenges. In the following, we illustrate some issues, without being exhaustive.

First, a State conducting a legal review needs to determine against which legal standards it reviews a cyber tool. In other words, the State will need to have answers to some of the questions discussed above, such as whether the use of a tool will qualify as an attack and is therefore subject to a broad range of IHL rules. For matters where the law is unclear or unsettled, a cautious approach may be warranted to avoid the subsequent appearance that the employment of a cyber tool was, or should have been deemed, unlawful.

Second, a State needs to determine what needs to be reviewed. This may not necessarily be evident with regard to cyber tools or cyber capabilities, as shown by the widespread use of these terms instead of notions such as cyber weapons. Commentators have discussed whether and which cyber tools or capabilities are weapons, means or methods of warfare, and what the implications are with respect to their legal review.[214] In any case, as noted above, States party to AP I must review all cyber tools or capabilities that qualify as weapons, means or methods of warfare. For States that are not party to AP I, the obligation to respect and ensure respect for IHL by their armed forces and the newness of the use of cyber technologies as weapon, means or method of warfare would make it

209 AP I, Art. 36.

210 See common Article 1; ICRC Customary Law Study, above note 63, Rule 139.

211 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006, p. 1.

212 *Ibid.*, pp. 22–23.

213 See ICRC Customary Law Study, above note 63, Rule 71. For an illustration of some of the issues raised by the legal review of cyber weapons, see "Scenario 10: Cyber Weapons Review", in K. Mačák, T. Minárik and T. Jančárková (eds), above note 68.

214 Jeffrey T. Biller and Michael N. Schmitt, "Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare", *International Law Studies*, Vol. 95, 2019, p. 219.

prudent to cast as large a net as possible in terms of the capabilities being reviewed.[215]

Third, a weapon or means of warfare should not be assessed in isolation from the way in which it will be used, meaning that the normal or expected use of the weapon or means of warfare must be considered in the legal review. Military cyber capabilities might, however, be less standardized than kinetic weapons, especially if designed for a specific operation. This would mean that the review needs to be done in view of the specific cyber environment in which the weapon will likely be used.

Fourth, and relatedly, a State should conduct a legal review not only for a weapon, means or method of warfare it intends to acquire or adopts for the first time, but also when it modifies a weapon, means or method that has already passed a legal review. This may pose a challenge with regard to cyber tools that are likely to be subject to frequent adaptation, including to respond to the software security upgrades that a potential target undergoes. While the question of the type and extent of change that would require a new legal review might need to be further clarified, a new legal review must be conducted, notably, when the weapon, means or method of warfare is modified in a way that alters its function or when the modification could otherwise have an impact on whether the employment of the weapon, means or method would comply with the law.[216] It has been noted in this respect with regard to cyber weapons that "the assessment of whether a change will affect a program's operation must be qualitative rather than quantitative in nature".[217] For legal reviews to be effective, States that study, develop, acquire or adopt new weapons, means or methods relying on new technologies need to navigate these and other complexities. In other words, testing regimes must adapt to the unique characteristics of cyber technology. In light of the above-mentioned complexities, a good practice to ensure respect for IHL by all States would be to share information about a State's legal review mechanisms and, to the extent feasible, about the substantive results of legal reviews.[218] This would be especially important where problems of compatibility of a weapon with IHL arise, in order to avoid other States encountering the same problems and to notify other States of the testing State's conclusions that such tools are prohibited by IHL. Exchange of information on legal reviews of weapons, means or methods relying on new technologies can also help build expertise and facilitate the identification of good practices, which may

215 For example, while the US DOD had the policy of carrying out legal review of weapons, including weapons that employ cyber capabilities (DoD Law of War Manual, above note 87, para 16.6), the relevant US Air Force instruction mandates the review of weapons and cyber capabilities: US Department of the Air Force, *Legal Reviews of Weapons and Cyber Capabilities*, Air Force Instruction 51-402, 27 July 2011.

216 ICRC, above note 211, p. 10.

217 Gary D. Brown and Andrew O. Metcalf, "Easier Said than Done: Legal Reviews of Cyber Weapons", *Journal of National Security Law and Policy*, Vol. 7, 2014, p. 133.

218 This has been proposed in the introductory remarks delivered by Helen Durham, Director of International Law and Policy of the ICRC, during the 22 January 2019 public hearing conducted by the Global Commission on the Stability of Cyberspace (statement on file with the ICRC).

assist States that wish to establish or strengthen their own legal review mechanisms.[219]

Conclusion

For the protection of the civilian population and civilian infrastructure in armed conflict, it is fundamentally important to recognize that cyber operations conducted during armed conflicts do not occur in a legal void but are regulated by international law, most notably IHL. As this article shows, recognizing IHL applicability is, however, not the end of the conversation. More discussion – in particular among States – is needed on how IHL is to be interpreted in cyberspace. Any such discussion should be informed by an in-depth understanding of the development of military cyber capabilities, the potential human cost they may cause, and the protection afforded by existing law. This article is meant to provide a basis for such discussions. While the use of cyber operations during armed conflicts, their potential human cost and States' legal positions on the subject are evolving, the analysis in this article presents a number of conclusions.

First, cyber operations during armed conflicts are a reality in today's armed conflicts and their use is likely to increase in the future. They can cause significant harm to the civilian population, especially if affecting critical civilian infrastructure such as medical facilities, electricity, water or sanitation. While the risk of causing human harm does not appear extremely high based on current observations, especially considering the destruction and suffering that conflicts always cause, the evolution of cyber operations requires close attention due to existing uncertainties and the rapid pace of change.

Second, in the ICRC's view, there is no question that cyber operations during armed conflicts are regulated by IHL – just as is any weapon, means or method of warfare used by a belligerent in a conflict, whether new or old. While the issue does not (yet) enjoy universal agreement, a careful examination of the various arguments raised in multilateral discussions shows that affirming IHL applicability legitimizes neither the militarization of cyberspace nor the use of malicious cyber operations. A State that considers carrying out a cyber operation against another State must analyze the lawfulness of this operation under the UN Charter and IHL. These two frameworks are complementary when it comes to the protection of humans from war and its effects. While some of the terminology they use is similar, the two frameworks are legally separate and require distinct analyses, as similar terminology has (at times) distinct meaning. For instance, concluding that a cyber operation triggers the applicability of IHL does not necessarily mean that it amounts to an armed attack giving rise to the right of self-defence.

219 ICRC Challenges Report 2019, above note 36, p. 35.

Third, the partly non-physical – i.e., digital – nature of cyberspace and the interconnectedness of military and civilian networks pose practical and legal challenges in applying the general IHL principles and rules protecting civilians and civilian objects. This is particularly the case with regard to the notion of "attack" under IHL, the question of whether civilian data enjoys similar protection as "civilian objects", and the protection of "dual-use" cyber infrastructure.

The question of whether or not an operation amounts to an "attack" as defined in IHL is essential for the application of many of the rules deriving from the principles of distinction, proportionality and precaution, which afford critical protection to civilians and civilian objects. For many years, the ICRC has taken the position that an operation designed to disable a computer or a computer network during an armed conflict constitutes an attack as defined in IHL whether the object is disabled through destruction or in any other way. This view is also reflected in the positions of a number of States.

While many of the general rules on the conduct of hostilities are limited to acts amounting to attacks as defined in IHL, some IHL rules governing the conduct of hostilities apply to a broader set of operations. IHL includes a few rules that apply to all "military operations", such as the obligation to take constant care to spare civilians and civilian objects. Moreover, IHL defines specific rules protecting certain categories of persons and objects, such as objects indispensable to the survival of the civilian population, medical services, and humanitarian relief operations. The protection they afford goes beyond the general protection afforded to civilians and civilian objects.

The protection of data against malicious cyber operations during armed conflict is becoming increasingly important because data is an essential component of the digital domain and a cornerstone of life in many societies. In the ICRC's view, the conclusion that cyber operations designed or expected to delete or tamper with essential civilian data would not be prohibited by IHL in today's ever more cyber-reliant world seems difficult to reconcile with the object and purpose of this body of norms, and raises significant concern.

In order to protect critical civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of cyberspace itself. It is traditionally understood that a civilian object may become a military objective when its use for military purposes is such that it fulfils the definition of military objective even if it is simultaneously used for civilian purposes. However, a party to a conflict that considers carrying out an attack against cyberspace infrastructure must analyze which distinct parts of the infrastructure make an effective contribution to military action, and whether their destruction or neutralization would, in the circumstances ruling at the time, offer a definite military advantage. Furthermore, this party must take all feasible precaution to avoid or at last minimize incidental civilian harm, including harm caused by indirect or reverberating effects, and must refrain from carrying out the attack if such harm may be expected to be excessive.

Fourth, in light of the particular challenges that the characteristics of cyberspace pose to the interpretation and application of some IHL principles in the conduct of hostilities, parties to armed conflicts who choose to develop, acquire or adopt weapons, means or methods of warfare relying on cyber technology need to exercise care in doing so. While legal reviews of new weapons, means and methods of warfare are mandatory for States party to AP I, legal reviews are critical for all States to ensure that their armed forces only use weapons, means or methods of warfare that comply with the State's obligations under IHL.

To conclude, recognizing that IHL applies in cyberspace and engaging in discussions on how it addresses the various challenges posed by the specific characteristics of the cyber domain and whether existing law is adequate and sufficient does not exclude that new rules might be useful or even needed. In our view, the answer to this question depends notably on how States interpret existing IHL obligations. If narrow interpretations are adopted, significant gaps in the protection of civilian populations and infrastructure may arise, and the existing legal framework might need strengthening. If new rules are developed, however, in our view it is critical that they build on and strengthen the legal framework that already exists – in particular IHL.