International Review of the Red Cross (2020), **102** (913), 335–365.
Digital technologies and war
doi:10.1017/S1816383121000023

IRRC

The application of the principle of distinction in the cyber context: A Chinese perspective

Zhixiong Huang and Yaohui Ying*
Zhixiong Huang is a Changjiang Outstanding Young Scholar Professor at the Wuhan University Institute of International Law/Institute for Cyber Governance, and a Research Fellow at the East China University of Political Science's Shanghai Key Innovation Team – Research of Legal Safeguard Mechanisms for the Belt and Road Construction. Email: fxyhzx@whu.edu.cn.

Yaohui Ying is a PhD candidate at Wuhan University Law School, China. Email: yingyaohui@whu.edu.cn.

Abstract
Up to now, the Chinese government has only made very general comments on the application of international humanitarian law to cyberspace. There are indeed Chinese academic papers concerning this issue, but the discussion of the principle of distinction is limited both in length and in academic depth. Compared with the West, research by Chinese scholars on this topic is still in a relatively preliminary stage. At present, there is no specific deconstruction or clarification of the application of the principle of distinction in cyberspace in Chinese academia. As

* This research is supported by the Major Projects of National Social Science Fund of China (Grant No. 20&ZD204). The authors are grateful to all the editors and anonymous referees for their useful suggestions and to Eric Jensen, Kubo Mačák, Ignacio de la Rasilla del Moral, Jinyuan Su, Nicole Hogg and Nicholas Tsagourias for their helpful comments on earlier drafts of this article. An earlier draft of this article was submitted to the workshop "Law in Today's Hybrid Armed Conflicts" held by Brigham Young University in February 2019, and all the feedback and comments from participants are most sincerely appreciated.

the first paper written by Chinese scholars specifically devoted to this question, this piece provides a different perspective by injecting the positions of Chinese officials and the views of Chinese scholars. The authors aim to clarify whether the existing rules are still completely applicable in the cyber context, and if needed, to find out what kind of improvements and clarifications can be made. Weighing in on these debates, we argue that despite the potential technical challenges and uncertainties, the principle of distinction should be applied to cyberspace. It should also be carefully re-examined and clarified from the standpoint of preventing over-militarization and maximizing the protection of the interests of civilians. For human targets, the elements of combatant status identified in customary international law and relevant treaties are not well suited to the digital battlefield. Nevertheless, cyber combatants are still obligated to distinguish themselves from civilians. In applying the principle of distinction, we argue that it makes more sense to focus on substantive elements over formal elements such as carrying arms openly or having a fixed distinctive sign recognizable at a distance. In interpreting "direct participation in hostilities", the threshold of harm requires an objective likelihood instead of mere subjective intention; the belligerent nexus should be confirmed, and the causal link should be proximate. Applying the "cyber kill chain" model by analogy helps us to grasp the whole process of direct participation in hostilities during cyber warfare. For non-human targets, all military objectives must cumulatively fulfil both the "effective contribution" and "definite military advantage" criteria, which are equally indispensable. The same requirements apply to dual-use objects. Furthermore, certain data should fall within the ambit of civilian objects.

Keywords: China, principle of distinction, cyberspace, cyber combatant, military objective, data.

Introduction

Up to now, the Chinese government has not been clear about the application of international humanitarian law (IHL)[1] to cyberspace. There have been some

1 In order to avoid confusion, a note is made at this point to clarify two terminologies, "law of armed conflict" (LOAC) and "international humanitarian law". There are some concerns about the inaccurate use of these two terms. Some think they have essentially the same meaning and can be used interchangeably, e.g. "the law of armed conflict, also known as international humanitarian law, includes principles such as distinction between military and civilian targets" (International Committee of the Red Cross (ICRC), *The Law of Armed Conflict: Basic Knowledge*, Geneva, June 2002, p. 2, available at: www.icrc.org/eng/assets/files/other/law1_final.pdf), while others render "international humanitarian law" as a potentially narrower concept that relates only to the laws in armed conflict that are designed to regulate the treatment of persons – civilian or military, wounded or active – in armed conflicts (Mary O'Connell, "Historical Development and Legal Basis", in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 11). There are also some critiques regarding the melding of battlefield laws and humanitarian goals, e.g. "a

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

preliminary debates concerning IHL in cyberspace among Chinese scholars,[2] especially those with a military background,[3] but the discussion of the principle of distinction in cyberspace is limited both in length and in academic depth. Compared with the West, research by Chinese scholars on this issue is still in a relatively preliminary stage, and some doctoral theses on the application of IHL to cyberspace are under way. At present, there is no specific deconstruction or clarification of the application of the principle of distinction in cyberspace in Chinese academia.

As the first paper written by Chinese scholars specifically devoted to the application of the principle of distinction in cyber warfare, this piece provides a

possible disadvantage of the term [IHL] is that it could be thought to exclude some parts of the laws of war (such as the law on neutrality) whose primary purpose is not humanitarian" (Jean Pictet, *Humanitarian Law and the Protection of War Victims*, A. W. Sijthoff, Leiden, 1975, p. 11). The International Law Commission distinguishes between LOAC and IHL, with the former governing the conduct and consequences of armed conflict while the latter forms part of the former and constitutes the *lex specialis* governing the conduct of hostilities (para. 4 of the Commentary to Art. 2 of the Draft Articles on the Effects of Armed Conflicts on Treaties, *ILC Yearbook*, Vol. 2, Part 2, 2011). For more detailed discussion on the terminology, see Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, Cambridge and New York, 2010, pp. 22–26. Chinese textbooks and papers generally hold the view that the term IHL has evolved from the law of war or LOAC, and thus treat them as synonymous; see, for example, 朱文奇, 何谓国际人道法, 武大国际法评论, 2003, 1 (Wenqi Zhu, "What Is International Humanitarian Law?", *Wuhan University International Law Review*, Vol. 1, 2003, only available in Chinese). For the purpose of this paper, the term "IHL" will be used generally, while the term "law of armed conflict" is used when the cited sources use that particular term.

2 See, for example, Li Zhang, "A Chinese Perspective on Cyber War", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, p. 804, available at: https://international-review.icrc.org/sites/default/files/irrc-886-zhang.pdf (all internet references were accessed in January 2021); Longdi Xu, "The Applicability of the Laws of War to Cyberspace: Exploration and Contention", 2014, p. 7, available at: www.gov.uk/government/publications/the-applicability-of-the-laws-of-war-to-cyberspace-exploration-and-contention; Chris Wu, "An Overview of the Research and Development of Information Warfare in China", in Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright (eds), *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave Macmillan, London, 2006; 朱莉欣, 信息网络战的国际法问题研究, 河北法学, 2009, 27(01) (Lixin Zhu, "Research on the International Law of Information Network Operations", *Hebei Law Science*, Vol. 27, No. 1, 2009, only available in Chinese); 姜世波, 网络攻击与战争法的适用, 武大国际法评论, 2013, 16(02) (Shibo Jiang, "War by Internet Cyber Attack and the Application of the Law of War", *Wuhan University International Law Review*, Vol. 16, No. 2, 2013, only available in Chinese); 李伯军, 论网络战及战争法的适用问题, 法学评论, 2013, 31(04) (Bojun Li, "On Cyber Warfare and the Application of the Law of War", *Law Review*, Vol. 31, No. 4, 2013, only available in Chinese); 朱莉欣, 平战结合与网络空间国际规则制定, 信息安全与通信保密, 2018(07) (Lixin Zhu, "Competition for International Rules in Cyberspace under the Combination of Peacetime and Wartime", *Information Security and Communications Privacy*, No. 7, 2018).

3 王海平, 武装冲突法研究进展及需要关注的问题, 当代法学, 2012, 26(05) (Haiping Wang, "The Research Progress of the Law of Armed Conflict and the Issues Needing Attention", *Contemporary Law Review*, Vol. 26, No. 5, 2012, only available in Chinese); 李莉, 鲁笑英.浅析信息化战争条件下武装冲突法所面临的问题, 西安政治学院学报, 2012, 25(01) (Li Li and Xiaoying Lu, "A Brief Analysis of the Problems Faced by the Law of Armed Conflict under the Condition of Information-Based Warfare", *Journal of Xi'an Politics Institute of PLA*, Vol. 25, No. 1, 2012, only available in Chinese); 朱雁新, 计算机网络攻击之国际法问题研究, 中国政法大学, 2011 (Yanxin Zhu, "The Research on the International Issues of Computer Network Attack", doctoral diss., China University of Political Science and Law, 2011, only available in Chinese); 张天舒, 从 "塔林手册" 看网络战争对国际法的挑战, 西安政治学院学报, 2014, 27(01) (Tianshu Zhang, "The Challenges of Cyber Warfare to International Law: From the Perspective of The Tallinn Manual on the International Law Applicable to Cyber Warfare", *Journal of Xi'an Politics Institute of PLA*, Vol. 27, No. 1, 2014, only available in Chinese).

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

different perspective by injecting the positions of Chinese officials and the views of Chinese scholars into the discussion. The authors hold the view that although States have vastly differing interpretations of exactly how IHL applies to cyberspace, the core principle of distinction is definitely applicable in cyberspace. This paper aims to clarify whether the existing rules are still completely applicable in cyber warfare, and if needed, to find out what kind of improvements and clarifications can be made. Given this, the first part introduces the *status quo* of the application of IHL to cyberspace and illuminates the Chinese official attitude alongside Chinese academic opinions on this issue. Subsequently, the second part reviews the concept of the principle of distinction and points out the contentious challenges of its application in the cyber context. Applying the persons–objects dichotomy, the third and fourth parts examine the substantive legal challenges involved and inject the relevant Chinese views. From the perspective of human targets, the third part analyzes the application of traditional criteria for defining who can be attacked in the cyber battlefield, identifies the relevant obstacles and makes corresponding suggestions. The fourth part focuses on non-human targets and discusses what can be attacked in cyber warfare – namely, what constitutes a military objective. It further addresses the Chinese scholarship on whether digital data *per se* is an object. The final part offers some preliminary concluding observations.

It is beyond doubt that the peaceful use of the cyberspace domain is of great importance to the common well-being of mankind. Fortunately, to date the world has remained free of any catastrophic mass-casualty cyber attacks, or equivalent catalysts for war such as a "cyber Pearl Harbor"[4] situation. However, the increasingly disturbing occurrence of belligerent cyber incidents, such as the inclusion of cyber means and methods in armed conflicts, are forcing us to pay close attention to the application of IHL in cyberspace.

Cyber warfare,[5] despite having the potential to allow for some level of anonymity on an *ad hoc* basis and a sense of interconnectedness, is still a kind of

4 James J. Wirtz, "The Cyber Pearl Harbor", *Intelligence and National Security*, Vol. 32, No. 6, 2017; James J. Wirtz, "The Cyber Pearl Harbor Redux: Helpful Analogy or Cyber Hype?", *Intelligence and National Security*, Vol. 33, No. 5, 2018; US Department of Defense (DoD), "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City", 12 October 2012, available at: https://content.govdelivery.com/accounts/USDOD/bulletins/571813.

5 In this article, the term "cyber warfare" is understood as "means and methods of warfare that rely on information technology and are used in the context of an armed conflict". See Jakob Kellenberger, "International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, Sanremo, Italy, 8–10 September 2011: Keynote Address by Dr Jakob Kellenberger", *International Review of the Red Cross*, Vol. 94, No. 886, 2012, available at: https://international-review.icrc.org/sites/default/files/irrc-886-kellenberger-spoerri.pdf. For some Chinese scholars, cyber warfare is a special form of information warfare and is a new means or method of warfare. Information warfare refers to a series of hostile activities carried out by belligerent parties in order to maintain their right to acquire, control and use information. Its connotation and extension are broader than cyber warfare and can include cyber warfare, intelligence warfare, electronic warfare, psychological warfare, etc. Cyber warfare refers to the process of disrupting, destroying or threatening the other belligerent parties' information and network systems while ensuring the security of one's own information and network systems through computer networks. See, for example, B. Li, above note 2. Some argue that the main question expressed by the concept of cyber warfare is whether

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

warfare. As such, multilateral discussions have been ongoing for over a decade now concerning whether IHL – as "the set of rules that seeks to limit the effects of armed conflicts"[6] – applies to the cyberspace domain. No consensus has been reached yet. There seemed to have been a glimmer of hope in the report of the 2014/15 United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, since it had already mentioned the applicability of the principles of distinction and proportionality in cyberspace:[7] the wording "international legal principles, including the principle of distinction"[8] is seen as a compromise because some States (presumably including China) do not wish to refer directly to the term IHL.[9] However, the subsequent 2016/17 UN GGE failed to arrive at a consensus, and one of the controversial issues concerned the application of IHL in cyberspace.[10] With the adoption of two separate (some may say competing) resolutions by the First Committee of the General Assembly in 2018,[11] the future for States' consensus on IHL in cyberspace seems more and more uncertain and confusing.

In an ideal world, it seems that once a situation has reached the threshold of an armed conflict, the application of *jus in bello* rules to cyberspace should be nothing more than putting old wine into a new bottle. If cyber warfare is merely a new means or methods of warfare, then the existing *jus in bello* rules would automatically apply, and there is nothing mysterious or inscrutable about it. However, the reality often runs counter to the ideal. Due to the huge difference between cyber and traditional battlefields, many existing rules appear to be rather confusing in cyber warfare, and must be re-conceptualized. This is especially true in the case of the principle of distinction. For instance, an important issue relating to this principle is that of distinguishing between cyber combatants and civilians. Combatants are obligated to carry arms openly and to have a fixed

cyber attackers "armed" with keyboards, computer viruses and malware can become (or have become) a new means or method of warfare. See 黄志雄主编, 网络空间国际规则新动向: "塔林手册 2.0 版"研究文集, 社会科学文献出版社, 2019: 301 (Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, p. 301); 黄志雄, 国际法视角下的 "网络战" 及中国的对策——以诉诸武力权为中心, 现代法学, 2015, 37(05) (Zhixiong Huang, "International Legal Issues concerning 'Cyber Warfare' and Strategies for China: Focusing on the Field of *Jus ad Bellum*", *Modern Law Science*, Vol. 37, No. 5, 2015).

6 See ICRC, "War and Law", available at: www.icrc.org/en/war-and-law.

7 See UN GGE, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174, 22 July 2015, para. 28, available at: www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

8 *Ibid.*

9 Michael N. Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", *Just Security*, 30 June 2017, available at: www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

10 See, for example, *ibid.*; Arun Mohan Sukumar, "The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?", *Lawfare*, 4 July 2017, available at: https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well.

11 See "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased", *Council on Foreign Relations Blog*, 15 November 2018, available at: www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased. The two resolutions are sponsored by Russia (UN Doc. A/C.1/73/L.27/Rev.1) and the United States (UN Doc. A/C.1/73/L.37) respectively.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

distinctive sign recognizable at a distance.[12] This is apparently not practical in the cyber context, where anonymity is often the norm and it is impossible to tell who is sitting in front of the computer that is implementing an attack. The rules were drafted in an era when warfare involved a certain amount of physical proximity between opposing forces; for the most part, combatants could see one another and hence distinguish between combatants and non-combatants, friends and foes.[13] When it comes to civilians who directly participate in hostilities,[14] the question becomes even more confusing. It is highly possible for unorganized individuals to launch cyber attacks against an adversary; the typical example would be a group of hacktivists performing a distributed denial-of-service (DDoS) attack for patriotic or ideological reasons. For instance, the anonymous cyber attack against Estonian essential infrastructures, telecommunications, DNS servers, websites and email servers in 2007 seemed to have followed a political row over the relocation of a Soviet "Monument to the Liberators of Estonia", which represents the USSR's victory over Nazism, from the centre of Tallinn to a military cemetery on the outskirts of the city.[15] Is the person who inputs the malicious code, or the person who writes (but does not execute) the code, or the person who gives the order for the code to be written in the first place, the one directly taking part in hostilities?

As the country with the largest number of netizens and one which suffers from frequent cyber attacks,[16] China has been very active in promoting the rule of law in cyberspace. Yet, while it has been a State party to the Geneva Conventions[17]

12 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), Art. 4(A)(2); 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. 44(3); Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), pp. 14–17, available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1.

13 Heather Harrison Dinniss, "Participants in Conflict – Cyber Warriors, Patriotic Hackers and the Laws of War", in Dan Saxon (ed.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff, Boston, MA, and Leiden, 2013, p. 256; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, Cambridge, 2012, p. 145.

14 The ICRC Customary Law Study, above note 12, Rule 6, stipulates that civilians are protected against attack unless and for such time as they take a direct part in hostilities. For substantive discussion about "direct participation in hostilities", see Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, ICRC, Geneva, 2009 (Interpretive Guidance).

15 For a detailed description of the cyber attack against Estonia in 2007, see "Cyber Attacks against Estonia (2007)", *International Cyber Law in Practice: Interactive Toolkit*, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), available at: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007); Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE, Tallinn, 2010, pp. 15–16, 31.

16 Chinese Academy of Cyberspace Studies (ed.), *China Internet Development Report 2017*, Springer, Berlin, 2019, p. 107; 国家互联网应急中心, 2020 年上半年我国互联网网络安全监测数据分析报告, 2020 (National Computer Network Emergency Response Technical Team/Coordination Centre of China, *Analysis Report of China's Internet Network Security Monitoring Data in the First Half of 2020*, 2020, only available in Chinese), available at: https://tinyurl.com/y2lpzdh4; Ministry of Foreign Affairs of the People' Republic of China, "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on September 29, 2020", available at: https://tinyurl.com/y4xolw3g.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

and Additional Protocols I and II to the Geneva Conventions (AP I and AP II)[18] for many years, China has not had much enthusiasm on the issue of IHL in cyberspace and has always avoided addressing the issue of cyber warfare and the law applicable to it.[19]

China's reluctance to discuss the IHL issue in depth has been evidenced on many occasions. For instance, in its recent submission to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, China stated that "the applicability of the law of armed conflicts and *jus ad bellum* needs to be handled with prudence";[20] this suggests that China, for some (maybe political) reason, does not want to discuss the details of IHL in cyberspace and therefore delays any clarification of the issue. Instead of specifying its position and rationale, China has only repeatedly affirmed that "the lawfulness of cyber warfare should not be recognized under any circumstance".[21] This resistant attitude is prominent in the speech given by the Chinese delegate at the 2019 Annual Session of the Asian–African Legal Consultative Organization (AALCO):

> China sticks to the principle of peaceful use of cyberspace and firmly opposes … cyber warfare or [the] cyber arms race. … Without 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. Given the "digital gap" between developing and … developed countries, developing countries in general will be in a disadvantaged position in the discussion and development of such rules, [and] it will be difficult to ensure the rules are fair and equitable.[22]

China attaches great importance to the peaceful use of cyberspace, and asserts that too much discussion of the application of IHL would have potential negative impacts on international peace and security, aggravating an arms race and the militarization of cyberspace. For instance, China has expressed its criticism by saying that "this military paradigm"[23] disregards the principle of non-use of

17 China's date of ratification/accession to the Geneva Conventions is 28 December 1956. See the ICRC Treaty Database, available at: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=CN.

18 China's date of ratification/accession to AP I and AP II is 14 September 1983. See *ibid.*

19 Binxin Zhang, "Cyberspace and International Humanitarian Law: The Chinese Approach", in Suzannah Linton, Tim McCormack and Sandesh Sivakumaran (eds), *Asia-Pacific Perspectives on International Humanitarian Law*, Cambridge University Press, Cambridge, 2019, p. 323.

20 See "China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security", p. 6, available at: www.un.org/disarmament/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

21 *Ibid.*

22 AALCO, *Verbatim Record of Discussions: Fifty-Eighth Annual Session*, AALCO/58/DAR ES SALAAM/2019/VR, Dar es Salaam, 21–25 October 2019, available at: www.aalco.int/Final%20Verbatim%202019.pdf.

23 AALCO, *Verbatim Record of Discussions: Fifty-Fourth Annual Session*, AALCO/54/BEIJING/2015/VR, Beijing, 13–17 April 2015.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

force[24] and may affect strategic trust between countries and increase the risk of inter-State misperception and conflict.[25] In this context, it is not surprising that the government of China has not been clear about the application of the principle of distinction in cyberspace. China's conservative attitude is understandable to some extent. Firstly, there is no widely recognized national practice that constitutes a cyber attack; secondly, due to the hysteretic nature of law, IHL in cyberspace should not be determined too early.[26] The existing negative attitude of the Chinese government on this issue may also be a delaying tactic in the process when China has not come up with a self-explanatory plan. From the authors' point of view, there is no legal obstacle to the application of IHL in cyberspace, especially the principle of distinction. It is undeniable that cyber warfare has already taken place and will continue to do so. Whether China likes it or not, it will probably have to express its stance on IHL in cyberspace.

The principle of distinction and the challenge of applying it to cyberspace

Having introduced the *status quo* of the application of IHL in cyberspace, China's official attitude, and some Chinese scholars' views on this point as the starting point of our analysis, it is now time to review the principle of distinction *per se* and summarize the contentious challenges of its application in the cyber context. The principle of distinction, according to the International Court of Justice (ICJ) in its *Legality of the Threat or Use of Nuclear Weapons* advisory opinion, is a cardinal principle of the law of armed conflict and has achieved the status of customary international law.[27] Article 48 of AP I stipulates that parties to a conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives, and shall accordingly direct their operations only against military objectives.[28]

Generally speaking, the principle of distinction takes a two-pronged approach to the regulation of hostilities. It prohibits indiscriminate means and methods of warfare, and it also regulates the use of those means and methods that are lawful – meaning that a distinction shall be made between military objectives and combatants, on the one hand, and other persons and objects that should be respected and protected, on the other. Indiscriminate attacks are prohibited.[29]

24 Xinmin Ma, "What Kind of Internet Order Do We Need?", *Chinese Journal of International Law*, Vol. 14, No. 2, 2015. Xinmin Ma served as deputy director of the Department of Treaty and Law of the Ministry of Foreign Affairs of China from 2014 to 2019.

25 AALCO, *Verbatim Record of Discussions: Fifty-Fifth Annual Session*, AALCO/55/NEW DELHI (HEADQUARTERS)/2016/VR, New Delhi, 17–20 May 2016.

26 For more explanation on China's attitude towards IHL, see B. Zhang, above note 19.

27 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, *ICJ Reports 1996*, p. 266.

28 AP I, Art. 48; ICRC Customary Law Study, above note 12, Rules 1, 7, pp. 3, 25.

29 AP I, Art. 51(4); ICRC Customary Law Study, above note 12, Rule 11, p. 37.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

An "attack" triggers a wide array of legal protections concerning distinction, especially those contained in Articles 49–58 of AP I. Therefore, in order to clarify exactly how the principle of distinction can be applied to cyberspace, a proper definition of "cyber attack" is a prerequisite. There have been some in-depth and meaningful academic discussions on what constitutes a cyber attack.[30] The most widely accepted definition takes a consequence-based approach. For example, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual 2.0) defines a cyber attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[31] We take this definition in this article.[32] No apparent legal provision explicitly bans or addresses the use of cyber warfare, as distinct from other forms of warfare. IHL is currently silent on distinction matters in cyber warfare, and some scholars therefore argue that the existing treaty-based framework is ill-suited to cope with it; this aspect of virtual war negatively affects the application of the principle of distinction.[33] One reason for this, as some scholars contend,[34] is that civilian and military infrastructures are not only closely interrelated and interconnected but are, in fact, one and the same thing. This assertion can lead to conclusions that pose significant obstacles to the application of the principle of distinction. If most components of cyberspace – such as fibre-optic cables, satellites, routers and nodes – are dual-use objects, simultaneously serving both military and civilian purposes, the classification of these objects can be problematic, leading to tricky

30 See Marco Rossini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 178–182; William H. Boothby, "Where Do Cyber Hostilities Fit in the International Law Maze?", in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict*, Springer, Berlin, 2014, pp. 60–62; Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks", paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17–19 November 2004; 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; Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?", *Stanford Law and Policy Review*, Vol. 25, No. 2, 2014.

31 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 92, p. 415.

32 The consequence-based approach is very useful as it switches the focus from the means and nature of an act to the effect and consequence of an act, thus fulfilling the requirement of "violence" and keeping the provision dynamic and evolutive. However, the present authors still have two concerns. The first is that from a practical perspective, the assessment of the damage turns out to be extremely tricky, especially when the consequences are mostly indirect. The second concern is that the consequence-based approach limits the notion of attack so as to exclude those operations that result in severe and disruptive non-physical harm. Similar concerns can be found in ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Geneva, November 2019 (ICRC Cyber Operations Paper), pp. 7–8. The ICRC has also mentioned that 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 is to ensure the protection of the civilian population and civilian objects against the effects of hostilities. See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 32IC/15/11, October 2015 (ICRC Challenges Report 2015), p. 41.

33 See Jeffrey Kelsey, "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", *Michigan Law Review*, Vol. 106, No. 7, 2008, pp. 1429–1430.

34 Robin Geiss and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space", *Israel Law Review*, Vol. 45, No. 3, 2012, pp. 381, 383.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

issues concerning the principle of proportionality.[35] At the same time, the classification of individuals as combatants or civilians is not always clear given that the mounting phenomenon of civilianization of war,[36] characterized by the increasing use of sophisticated cyber technologies, has blurred the contours. Militaries and civilian enterprises are communicating, cooperating and integrating at an unprecedented depth.[37] For instance, China has twice included the strategy of civil–military integration in its white papers.[38] Also, the attribution of responsibility presents difficulties;[39] while it is mostly easy to see where a missile was launched from, the deployment of cyber operations doesn't create smoke plumes.

Several scholars have made a rigorous effort to research how the principle of distinction applies in cyber warfare,[40] and several states, such as the United States[41] and Denmark,[42] have added the principle of distinction's application in cyber warfare into their respective Military Manuals. It is generally agreed, for instance, that an attack does not have to be kinetic for IHL rules to apply to it; that indiscriminate attacks[43] are prohibited; and that if an attack does not specifically target any particular military persons or objects, it shall never be permitted. This could be the case with a computer virus, if it can spread uncontrollably from military systems to connected civilian systems. While there is a consensus that a distinction must be made between military objectives/combatants and civilian objects/civilians, when it comes to the more practical level of exactly what constitutes a military objective and who is a combatant in a cyber armed conflict, the question becomes extremely controversial. Moreover, as raised by one Chinese scholar, the non-lethal underlying feature of cyber means and methods makes traditionally protected objects and individuals more

35 The principle of distinction provides that only military objectives may be directly targeted in armed conflict. However, an attack on a legitimate military objective may sometimes cause incidental damage to civilian persons or objects. These harmful side effects are regulated by the principle of proportionality, which prohibits attacks that may be expected to cause injury to civilian life or property that is excessive in relation to the anticipated military advantage. A clear statement of the principle of proportionality can be found in AP I, Art. 51(5)(b). See also Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law*, Edward Elgar, Cheltenham, 2013, pp. 55–57.

36 "Civilians play an increasingly important and complex role in armed conflicts, both as victims and perpetrators." This overall trend is called "civilianization" in Andreas Wenger and Simon J. A. Mason, "The Civilianization of Armed Conflict: Trends and Implications", *International Review of Red Cross*, Vol. 90, No. 872, 2008.

37 L. Zhu, "Competition for International Rules in Cyberspace", above note 2, p. 40.

38 State Council Information Office of the People's Republic of China (SCIO), *China's National Defense in the New Era*, Beijing, July 2019, available at: www.scio.gov.cn/zfbps/32832/Document/1660325/1660325.htm; SCIO, *China's Military Strategy*, Beijing, May 2015, available at: www.scio.gov.cn/zfbps/ndhf/2015/Document/1435159/1435159.htm.

39 See ICRC Cyber Operations Paper, above note 32, pp. 8–9.

40 See, for example, J. Kelsey, above note 33, p. 1427; Yoram Dinstein, "The Principle of Distinction and Cyber War in International Armed Conflicts", *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 261; Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *Jus in Bello*", *International Review of the Red Cross*, Vol. 84, No. 846, 2002, p. 365.

41 DoD, *Law of War Manual*, Washington, DC, 12 June 2015, pp. 985–999.

42 Danish Ministry of Defence, Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Copenhagen, September 2016.

43 AP I, Art. 51(4).

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

vulnerable in cyber warfare than in conventional warfare. This will lead to confusion in evaluating the legitimacy of cyber operations and make the principle of distinction more frequently violated in cyber military operations.[44] Given the significance of the principle of distinction on the cyber battlefield, it is necessary to clarify whether the existing rules are still completely applicable in cyber warfare, and to find out what kind of improvements and clarifications can be made.

The principle of distinction concerning human targets in cyber warfare

The principle of distinction follows a persons–objects dichotomy to define the nature of the target. No matter how cyber technology evolves, the perpetrator of a hostile act is still a person, and even when planting viruses or attacking firewalls in ways that look like mere keystrokes and mouse clicks, the persons–objects dichotomy, which defines "who" and "what" can be attacked, still applies. This part of the article will deal with the issue of who can be lawfully attacked in the cyber context. The foundational principle is that civilians shall not be the object of attack.[45] The principle of distinction assumes that belligerents can clearly distinguish between civilians and combatants; the anonymity of cyberspace, however, makes this assumption hard to maintain.

Every combatant is a former civilian, and any civilian may convert himself into a combatant,[46] either by being conscripted or volunteering to join the armed forces of a belligerent party, or by taking a direct part in hostilities (this leads to the loss of protected status while doing so),[47] or by becoming part of a *levée en masse*, a concept that allows the transition from civilians to lawful combatants.[48] The authors will not address *levée en masse* here, because this concept requires the physical invasion of national territory and the involvement of a large segment of population,[49] which is almost impossible by cyber means.[50]

Due to the advantages of easy denial of State responsibility and low cost, "the majority of cyber operations are outsourced to civilian cyber experts".[51] In

44 陈鹏飞, 论当代武装冲突法面临的挑战, 西安政治学院学报, 2014, 27(05) (Pengfei Chen, "Analysis of the Challenges to Contemporary Armed Conflict Law", *Journal of Xi'an Politics Institute of PLA*, Vol. 27, No. 5, 2014, only available in Chinese).

45 AP I, Art. 51(2); ICRC Customary Law Study, above note 12, Rule 6, pp. 19–24.

46 Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge University Press, Cambridge, 2016, p. 174.

47 AP I, Art. 51(3); ICRC Customary Law Study, above note 12, Rule 6, pp. 20–21; Interpretive Guidance, above note 14, pp. 41–68.

48 GC III, Art. 4A(6); ICRC Customary Law Study, above note 12, Rule 106, pp. 386–387, and in particular Rule 5, which explains that members of a *levée en masse* are an exception to the definition of civilians in that although they are not members of the armed forces, they qualify as combatants.

49 GC III, Art. 4A(6).

50 Tallinn Manual 2.0, above note 31, Rule 88, p. 409.

51 Elizabeth Mavropoulou, "Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks", *Journal of Law and Cyber Warfare*, Vol. 4, No. 2, 2015, p. 78.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

light of this trend, there is a high probability that, with the exception of cyber units incorporated into the regular armed forces, "many of the personnel substantively involved in cyber operations may actually be civilians".[52] Could a patriotic hacker or computer scientist thus become the object of an attack? The answer depends on the interpretation of "direct participation in hostilities" in the context of cyber operations.

Who is a cyber combatant?

Civilians who directly participate in hostilities lose their protected status and are not entitled to combatant immunity; some scholars even argue that they are "unlawful"[53] combatants. IHL encourages a clear and reliable division between combatants and non-combatants, and this reflects the fundamental role played by the principle of distinction in this body of law. Combatants have the right to participate directly in hostilities[54] and are subsequently immune from prosecution for acts which are carried out in accordance with IHL;[55] thus, they are targetable. Cyber warfare is no exception to this. Since the definition of civilians is a purely negative one (civilians are persons who are not combatants[56]), the question of who is a cyber combatant becomes a critical issue.[57]

It has been seen that some States have established special sections within their armed forces responsible for cyber operations. For instance, the United States has established US Cyber Command (USCYBERCOM), which was elevated from a sub-unit of the US Strategic Command to the status of a Unified Combatant Command,[58] while Colombia has created an Armed Forces Joint Cyber Command, tasked with preventing and countering cyber threats or attacks affecting national values and interests.[59] The definition of cyber combatant is worthy of discussion because it not only involves the issue of who is a legitimate target, but also has an impact on who is entitled to prisoner of war (PoW) status if captured.

52 David Turns, "Cyber Warfare and the Notion of Direct Participation in Hostilities", *Journal of Conflict and Security Law*, Vol. 17 No. 2, 2012, p. 292; see also Michael N. Schmitt, "'Direct Participation in Hostilities' and 21st Century Armed Conflict", in Horst Fischer and Dieter Fleck (eds), Crisis *Management and Humanitarian Protection: Festschrift for Dieter Fleck*, BWV, Berlin, 2004, p. 527.

53 Y. Dinstein, above note 46, p. 44.

54 AP I, Art. 43(2).

55 H. Harrison Dinniss, "Participants in Conflict", above note 13, p. 254.

56 AP I, Art. 50(1); ICRC Customary Law Study, above note 12, Rule 5, pp. 17–19.

57 Vijay M. Padmanabhan, "Cyber Warriors in the Jus in Bello", *International Law Studies*, Vol. 89, 2013; Maurizio D'Urso, "The Cyber Combatant: A New Status for a New Warrior", *Philosophy and Technology*, Vol. 28, No. 3, 2015; Jake B. Sher, "Anonymous Armies: Modern 'Cyber-Combatants' and Their Prospective Rights under International Humanitarian Law", *Pace International Law Review*, Vol. 28, No. 1, 2016; Sean Watts, "The Notion of Combatancy in Cyber Warfare", paper presented at the 4th International Conference on Cyber Conflict, Tallinn, 5–8 June 2012.

58 Donald Trump, "Statement by President Donald J. Trump on the Elevation of Cyber Command", 18 August 2017, available at: www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-elevation-cyber-command/.

59 UN, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, UN Doc. A/67/167, 23 July 2012, p. 5.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

Combatants are basically members of the armed forces of a belligerent party – whether these forces are regular or irregular, and irrespective of belonging to the standing army or to reservist units – including paramilitary militias incorporated *de facto* into the armed forces. The specific task assigned to an individual within the military apparatus is irrelevant.[60]

The Geneva Conventions have enumerated five conditions which must be satisfied for lawful combatant status.[61] The first four are cumulative conditions set out by the Hague Regulations and Geneva Conventions for the applicability of PoW and lawful combatant status: (i) being under the command of a person responsible for his or her subordinates (organization); (ii) having a fixed distinctive sign recognizable at a distance; (iii) carrying arms openly; and (iv) conducting operations in accordance with the laws and customs of war (compliance).[62] These four conditions apply to members of other militias and members of other volunteer corps, but they are also implicit requirements for members of the armed forces of a party to the conflict. An additional condition may be implied from the Geneva Conventions, which is (v) belonging to a party to the conflict.[63]

The authors believe that elements (i), (iv), and (v) are substantive elements, while elements (ii) and (iii) are formal ones. Considering the fact that anonymity is the normal status in cyber warfare, it makes more sense to focus on the substantive elements instead of the formal ones.

The first element, that of organization, is essential in cyber warfare. This is more of a factual issue than a legal one, and this requirement reflects the presence of a responsible command and a hierarchical relationship.[64] If a cyber group does not have sufficient organization, typically a superior–subordinate structure, division of duties and accountability, and certain elements of discipline and supervision, its members cannot be lawful combatants and certainly would not be entitled to combatant immunity. Given that members of most cyber groups have the same intention but lack common discipline, the chances that an armed group which exists exclusively online will be sufficiently organized are slim.[65] For instance, if no consequence will occur when members of a group suddenly decide to stop or not to participate in cyber hostilities (it may be the case that cyber group members do not know each other at all), or the members of a group do not feel compelled to follow the orders of a commander, it is not reasonable to submit

60 Y. Dinstein, above note 46, p. 41.
61 H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 144.
62 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), Art. 13(2); 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), Art. 13 (2); GC III, Art. 4(A)(2); 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), Art. 4(2); H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 145.
63 GC III, Art. 4A(6); H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 145.
64 Y. Dinstein, above note 46, p. 39; International Criminal Tribunal for Rwanda (ICTR), *The Prosecutor v. Jean-Paul Akayesu*, Case No. ICTR-96-4-T, Judgment (Trial Chamber), 2 September 1998, para. 626.
65 Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 195.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

that such a loosely organized group fulfils the element of organization. This is particularly true in the case of patriotic cyber groups.[66]

The fourth element, that of compliance with IHL, remains indispensable and has not changed markedly with the advent of computer network technology.[67] If combatants are themselves unwilling to respect IHL, they are prevented from relying on that body of law when desirous of reaping its benefits.[68]

The last element is that of belonging to a party to the conflict, which aims at proving a certain relationship between a group launching cyber attacks and a belligerent state.[69] While computer network attacks enable the use of "cyber militia" and offer the attractiveness of "plausible deniability" for a State, unless a relationship can be established between the group and the State, the participants will not be considered as lawful combatants.[70] The regular armed forces of the State would have no need to prove such a connection, but when it comes to organized online groups, it is not clear what degree of control over them is required.[71]

The most puzzling issue concerns the second and third elements, which require combatants to have a fixed distinctive sign recognizable at a distance and to carry arms openly. These two conditions are closely linked to the principle of distinction between combatants and civilians. Given that the two conditions are intended to eliminate confusion in this regard and to preclude any attempt at deception,[72] there is an inherent difficulty in transplanting them into an online environment, where it is impossible to tell who is sitting at any given computer due to the anonymity of cyberspace. Some scholars have proposed that given the impossibility of computer users being marked with distinctive signs, the requirement of displaying signs should be applied to computers or systems, just as military automobiles, aircraft and ships need to be marked with distinctive signs. This proposal is untenable since marking a military computer is tantamount to making a lawful target of any system to which it is connected.[73]

66 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.

67 H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 149.

68 Y. Dinstein, above note 46, p. 54.

69 See Denise Bindschedler-Robert, "A Reconsideration of the Law of Armed Conflicts", in *The Law of Armed Conflicts: Report of the Conference on Contemporary Problems of the Law of Armed Conflict*, 1971, p. 40; Katherine Del Mar, "The Requirement of 'Belonging' under International Humanitarian Law", *European Journal of International Law*, Vol. 21, No. 1, 2010.

70 H. Harrison Dinniss, "Participants in Conflict", above note 13, p. 262.

71 The effective control standard elaborated by the ICJ in Nicaragua appears inappropriate to define what "belonging to a party to the conflict" means, as, unlike the overall control and complete dependency standards, it expresses control over the act and not over the actor and thus focuses on specific activities. Marko Milanović, "State Responsibility for Acts of Non-State Actors: A Comment on Griebel and Plücken", *Leiden Journal of International Law*, Vol. 22, No. 2, 2009, p. 317. On the meaning of the effective control, overall control and complete dependency standards, see Antonio Cassese, "The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia", *European Journal of International Law*, Vol. 18 No. 4, 2007.

72 Y. Dinstein, above note 46, p. 37.

73 The Internet is constantly searched by millions of software bots intent on finding connected computers; a bot searching for military-designated IP addresses would be able to find them in a matter of minutes. Once

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

One may argue that armed forces could still wear uniforms in order to comply with the obligation of having a fixed distinctive sign recognizable at a distance;[74] for example, requiring members of USCYBERCOM to wear military uniforms when conducting cyber operations. This opinion apparently has merit – it would be ideal if regular forces could wear uniforms or otherwise distinguish themselves from civilians – but in practice such a requirement would probably mean little, since the warring parties remain anonymous. The object and purpose of this provision is that the aim of wearing a uniform is to eliminate the possibility of confusion in distinguishing between civilians and combatants. In traditional armed conflicts, by wearing uniforms, in most instances it is clear who is a combatant and who is not.[75] But when cyber combatants are sitting in front of their computers, sometimes a great distance from the view of those they are attacking, whether they wear uniforms or not makes no difference to the other belligerent State. In any event, even if we insist that formal military forces should wear uniforms, this requirement is absurd when dealing with cyber militias, volunteer corps or other organized cyber groups. What is more, it seems that cyberspace leaves no room for the requirement of carrying arms openly. Defining cyber weapons is already difficult enough, and to carry them openly is just impractical.[76] Certainly, it should not be ignored that there is a possibility of a kinetic attack on cyber combatants. In conclusion, we argue that in cyber warfare, the second and third elements would not be deleted outright, but there would be little need for much discussion about them.

Some may deem that on the digital battlefield, there is no real need for such distinctions; in the context of a cyber attack against military assets, the one who committed the attack is either a combatant or a civilian directly participating in hostilities. In either case, this specific person has lost his or her protected status. Nevertheless, some questions remain, particularly as to whether he or she would enjoy PoW status once captured.[77] Moreover, a civilian attacker might fail to meet the requirement of "threshold of harm" and "belligerent nexus",[78] and thus he or she would not lose the protected status at all.

identified, the only way to effectively move the computer or system out of range is to disconnect it, a solution which is likely to disrupt its normal running and/or usefulness; thus, any system remaining connected to the network in any way would be solely reliant on its electronic defences to prevent intrusions and defend against them. So, while initially the idea of displaying signs on computers or systems appears a useful solution, in practice it creates an imbalance between the purpose of the requirement of displaying signs and the ability of the military to conduct operations. See H. Harrison Dinniss, "Participants in Conflict", above note 13, p. 257; H. Harrison Dinniss, *Cyber Warfare*, above note 13, pp. 145–149.

74 Tallinn Manual 2.0, above note 31, Rule 87, p. 405.

75 This is not always the case; for example, civilians who directly participate in hostilities can be attacked, but they are hardly likely to wear military uniforms.

76 See Prashant Mali, "Defining Cyber Weapon in Context of Technology and Law", in Information Management Association, *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, PA, 2019; 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; H. Harrison Dinniss, *Cyber Warfare*, above note 13, pp. 250–278.

77 H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 148.

78 Interpretive Guidance, above note 14, p. 46.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

In conclusion, defining who is a cyber combatant is not only a legal intricacy, but also an extremely difficult technical issue for most States. The reality is that there is currently no way to clearly identify cyber combatants, and the existing rules are therefore applicable only to a limited extent. In comparison to a traditional armed conflict, civilians are more likely to be involved in a cyber armed conflict.[79] As Michael Schmitt has noted, the reasons for heavy civilian representation are multiple. From a cost-benefit perspective, training military personnel with cyber attack and defence expertise is extremely expensive and time-consuming for most countries, and what is more, the results are not guaranteed. In addition, cyber technology, by its nature, cannot be standardized and quantified. Not only is the technology always being developed and upgraded, it is also too limited and specialized.[80]

Elements (ii) and (iii) identified above – having a fixed distinctive sign recognizable at a distance and carrying arms openly – are ill-suited to the cyber context and thus probably need not be considered in cyber warfare. However, a person still has to at least satisfy elements (i), (iv) and (v) – the presence of a responsible command and a hierarchical relationship, conducting operations in accordance with the laws and customs of war, and belonging to a party to the conflict – to become a lawful combatant. Otherwise, they either remain protected from attack or will be considered as taking direct part in hostilities. Under these circumstances, the priority should be preventing over-militarization and minimizing unnecessary harm to civilians. Meanwhile, we should bear in mind that in case of doubt as to whether a person is a civilian, that person shall be considered to be a civilian.[81] Thus, it would be both unethical and unlawful to interpret the definition of cyber combatants in too broad a way.

Civilians taking direct part in cyber hostilities

Unlike combatants, civilians are not entitled to directly participate in hostilities; those who do so lose their general protection against the dangers of military operations and may be attacked for such time as they do so.[82] In addition, they may be prosecuted in domestic courts for their actions, even if the acts committed were lawful under IHL.[83] In the cyber context, the concept of civilians who directly participate in hostilities may be even more important, given the contemporary tendency in armed forces to outsource specialist work which requires cyber expertise to civilians.[84]

79 L. Zhu, "Competition for International Rules in Cyberspace", above note 2, p. 40.
80 M. N. Schmitt, above note 52, p. 527.
81 AP I, Art. 50(1); ICRC Customary Law Study, above note 12, Rule 6, pp. 23–24.
82 AP I, Art. 51(3); 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), Art. 13(3); ICRC Customary Law Study, above note 12, Rule 6, pp. 19–24.
83 H. Harrison Dinniss, "Participants in Conflict", above note 13, p. 258.
84 D. Turns, above note 52, p. 279.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

As discussed above, the term "direct participation in hostilities" refers to the notion that, as a general rule, civilians are not to be made the targets of attacks, unless and for such time as they directly participate in hostilities.[85] This is also known as the rule on non-combatant immunity.[86] When debating Article 51 of AP I, States did not settle on a precise definition of what was meant by the phrase "direct part in hostilities".[87] Both the *Targeted Killings* case[88] and the International Committee of the Red Cross's (ICRC) *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (Interpretive Guidance)[89] have made an important contribution to the interpretation of the notion of direct participation in hostilities. The Interpretive Guidance has generated considerable debate and some controversy.[90] While uncertainties remain and it is not crystal-clear how the guidance might be applied in practice on the physical battlefield, this is *a fortiori* the case when it comes to the virtual battlefield.[91]

Determining direct participation in hostilities is complex enough; determining direct participation in cyber hostilities seems even harder. As noted in the *Targeted Killings* case, it is possible to take part in hostilities without using weapons at all.[92] Thus, while the means of warfare today may be profoundly different from those of the last century, the effects of such means of warfare are essentially similar. A military communication system is rendered equally inoperative whether it is disabled by a computer virus or a bombing raid.

To further deconstruct this issue and provide guidance for practitioners, the Interpretive Guidance posits three cumulative elements which together constitute the act of direct participation in hostilities. First, the act must be likely to adversely affect the military operations of a party to an armed conflict or, alternatively, to inflict death, injury or destruction on persons or objects protected against direct attack (threshold of harm). Second, there must be a direct causal link between the act and the harm likely to result either from that act or from a coordinated military operation of which that act constitutes an integral part (direct causation). And third, the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).[93] Computer network attacks and computer network exploitation are also discussed, leading to the assessment that

85 AP I, Art. 51(3).
86 Judith G. Gardam, *Non-Combatant Immunity as a Norm of International Law*, Martinus Nijhoff, Dordrecht, 1993.
87 Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Dordrecht, 1982, pp. 301–304.
88 Israel High Court of Justice, *Public Committee against Torture in Israel v. Israel et al.*, Case No. HCJ 769/02, Judgment, 11 December 2005 (*Targeted Killings*).
89 Interpretive Guidance, above note 14, p. 46.
90 "Forum: Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance", *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010.
91 D. Turns, above note 52, p. 285.
92 Israel High Court of Justice, *Targeted Killings*, above note 88, para. 33.
93 Interpretive Guidance, above note 14, p. 46.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

"electronic interference with military computer networks could suffice as direct participation in hostilities, whether through computer network attacks or computer network exploitation, as well as wiretapping the adversary's high command or transmitting tactical targeting information for attack".[94] This three-part conjunctive test, focusing on the threshold of harm, direct causation and the belligerent nexus, provides a useful starting point for assessing whether and to what extent a civilian is conducting cyber combatant activities should thus lose their protected status.[95] It remains an open question whether these criteria are interpreted in the same way in the cyber context.

The first element, that of threshold of harm, relates to the objective likelihood of causing death or injury to humans or destruction to property. If, for example, both the 2007 Estonia incident[96] and the 2010 Stuxnet incident[97] had been perpetrated by civilians in an international armed conflict, we could conclude that the cyber attacks in the Estonia incident would have failed to reach the threshold of harm, while in the Stuxnet scenario, the attacks would have reached such a threshold. The cyber attacks against Estonian cyber infrastructure caused large-scale inconvenience since Estonia is one of the most "wired" States in the world, but no one died or was injured, nor was any property destroyed or damaged, and the causing of mere inconvenience, however unpleasant, does not reach the threshold of harm.[98] However, what is covered by "inconvenience" is not defined, and this terminology is not used in IHL.[99]

On the other hand, the cyber attack against the Iranian nuclear centrifuges, used for enriching uranium, caused physical damage to those centrifuges.[100] In this respect, the Tallinn Manual 2.0 dictates that "the act must have the intended or actual effect of negatively affecting the adversary's military operations or capabilities, or inflicting death, physical harm, or material destruction on persons or objects protected against direct attack".[101] Thus, as set out in the Manual, the threshold of harm element is met even if the acts merely have the intended effect. This interpretation expands the threshold of harm element from objective likelihood to either subjective intention or objective likelihood, and further leaves a lot of room for discretion on this point.

94 *Ibid.*, p. 48.
95 This three-part test has also been adopted for application to cyber warfare in the Tallinn Manual 2.0, above note 31, pp. 429–430.
96 "Cyber Attacks against Estonia (2007)", above note 15; E. Tikk, K. Kaska and L. Vihul, above note 15, pp. 14–33.
97 "Stuxnet (2010)", *International Cyber Law in Practice: Interactive Toolkit*, CCD COE, available at: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010); E. Tikk, K. Kaska and L. Vihul, above note 15, pp. 66–89.
98 D. Turns, above note 52, p. 286.
99 ICRC Challenges Report 2015, above note 32, p. 42.
100 A report shows that between the end of 2009 and early 2010, about 1,000 centrifuges at a fuel enrichment plant facility in Natanz, Iran, had to be replaced, implying that those centrifuges were broken. David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Institute for Science and International Security, 22 December 2010; "Stuxnet (2010)", above note 97.
101 Tallinn Manual 2.0, above note 31, p. 429.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

The second element, that of a direct causal link, should be interpreted broadly. According to the Interpretive Guidance, the harm in question must be brought about in "one causal step".[102] Such a strict interpretation of the causal proximity will be particularly problematic for cyber operations where the secondary or knock-on effect of a particular act may in fact be the purpose of the attack. We believe that "proximate causality", which contains both the subjective and objective perspective, is more suitable in the cyber context – that is to say, objectively, the damage caused by the cyber act is the normal and natural consequence, and such damage is subjectively foreseeable.[103]

Some hypothetical scenarios could help us better understand the proximate causality test in the cyber context. Civilians hired to perform general computer and IT services would not be deemed to be directly participating in hostilities if they were simply performing service contracts, such as running web pages and managing email log-in terminals,[104] because the causality is not proximate, any damage caused is not the normal and natural consequence of the actions involved, and any negative consequences may not be foreseeable by those carrying out the services. On the other hand, any employee or contractor who is specifically employed to conduct hostile cyber attacks would, in theory, satisfy the proximate causality test once he or she has done so.

It is also worth attempting to apply the "cyber kill chain" model,[105] which has been developed by Lockheed Martin to test whether there is proximate causality in specific conditions. The cyber kill chain model is an ordered list of the seven steps of a cyber attack, namely reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives.[106] It gives a bird's-eye view of how a hacker can strike a target, and although not every attack may adhere to all of these steps, it still provides a good starting point. The first phase is reconnaissance, which includes the research, identification and selection of targets; this followed by the weaponization phase, which couples malware and exploits into a deliverable payload. The next step, delivery, involves transmitting the weapon to the target (e.g., via USB drives or email attachments); subsequently, the weapon will try to exploit a vulnerability in order to gain access to the victim. Until the end of the fourth phase, it is still hard to say whether the acts have a direct causal link with the consequence, since what will happen next is not necessarily foreseeable for the perpetrators. However, when it comes to the installation, command and control, and action on objectives phases, there is a high chance that the perpetrator will be able to foresee what will happen, and the damage caused is the natural or normal consequence of the acts in question.

102 Interpretive Guidance, above note 14, p. 53.

103 Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge University Press, Cambridge, 1987, p. 181.

104 See Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare*, Sydney Law School Research Paper No. 12/10, 8 February 2012, available at: https://ssrn.com/abstract=2001794.

105 See Lockheed Martin, "Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense", 2015, available at: www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

106 *Ibid.*

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

The belligerent nexus element is more a matter of fact than of law. Certainly, it requires that "the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another".[107] It is not a *mens rea*-like element. What matters is the purpose of the act, which must be objectively designed to directly cause harm. This leads to the inference that hostile acts carried out under coercion or without knowledge will not satisfy the element of belligerent contact. In light of the fact that botnet attacks occur frequently, it must be noted that there should be an exemption to the loss of immunity if a civilian computer is hacked by a botnet and the relevant user is unaware of the virus and the attack. In this case, the relevant user should not be regarded as performing an action, and consequently, as they lack any manifestation of action, they would not fulfil the belligerent nexus element.

If a civilian merely writes a malware program which would result in the shutdown of critical infrastructures, this action should not be regarded as direct participation in cyber hostilities, since it would normally fail to satisfy all three elements, and in any case, the causality would be too remote. Similarly, civilian scientists and weapons experts are generally regarded as protected from direct attack.[108] If the civilian sends this self-written malicious program to the armed force that he or she supports, such action still does not constitute direct participation in hostilities – this is similar to the transportation of weapons. However, if this malicious program is aimed at conducting a specific hostile act, this action would become an integral part of a cyber military operation, thus fulfilling the proximate causality requirement. When a civilian, no matter whether they are under a contract with the armed forces or acting unilaterally, executes such a malicious program, they would probably fulfil the criteria and thus would lose their protected status and become a lawful target, at least during the period when the program was being executed.

Article 51 of AP I also stipulates the temporal scope of specific acts amounting to direct participation in hostilities – that is, civilians lose protection against direct attack "for such time" as they directly participate in hostilities.[109] If "such time" has passed, the protection granted to the civilian returns. This should be distinct from the rules set for members of armed wings of organized armed groups and for those who belong to a party to the conflict; these individuals are no longer civilians and, therefore, lose their protection against direct attack for the duration of their continuous combat function, while civilians lose their protection for the duration of specific acts amounting to direct participation in hostilities.[110]

107 Interpretive Guidance, above note 14, p. 46.

108 ICRC, *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report*, Geneva, 27–28 November 2006, p. 48. The present authors note that some doubts were expressed as to whether this assessment could be upheld in extreme situations – namely, those in which the expertise of a particular civilian is of very exceptional and potentially decisive value for the outcome of an armed conflict, such as the case of nuclear weapons experts during the Second World War.

109 AP I, Art. 51(3); ICRC Customary Law Study, above note 12, Rule 6, pp. 19–24.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

A particularly important issue in the cyber context is that of how to calculate the temporal scope of civilian loss of protection when dealing with repeated cyber operations in a relatively concentrated time period. If a civilian repeatedly launches cyber operations that could constitute direct participation in hostilities, what is the temporal scope, or period for that civilian of being targetable?

In a traditional battlefield setting, the Interpretive Guidance takes the position of treating those actions separately,[111] but the *Targeted Killings* case expresses concern about the "revolving door" phenomenon in this regard.[112] In the eyes of the Interpretive Guidance, the "revolving door" of civilian protection prevents attacks on civilians who do not, at the time, represent a military threat.[113] As the concept of direct participation in hostilities refers to specific hostile acts, IHL restores the civilian's protection against direct attack each time his or her engagement in a hostile act ends.[114] Considering that a large amount of cyber operations, such as DDoS attacks, are conducted multiple times within a time period, this strict time demarcation makes little operational sense. Yet the present authors also hold a sceptical attitude about calculating the period from the first operation throughout the whole intermittent activity. This is because civilians who directly participate in hostilities are not the same as members of organized military groups: though they are both targetable, they are two types of human targets. As mentioned before, members of organized military groups are targetable for the duration of their continuous combat function, but civilians who directly participate in hostilities are targetable only for the duration of their specific acts. "A civilian taking a direct part in hostilities one single time, or sporadically, who later detaches himself from that activity, is a civilian who, starting from the time he detaches himself from that activity, is entitled to protection from attack."[115] So, presuming that a civilian engages in repeated cyber attacks, if the whole period of time (from the beginning of the first attack to the end of the last attack) is continuously calculated as the period during which the civilian can be attacked, in a sense we are treating the civilian who directly participates in hostilities by the standard of combatants (continuous combat function), because we are directly regarding the intermission as an attackable period as well. Strictly speaking, civilians who directly participate in hostilities lose their protected status because of their specific acts, and are not considered to have carried out any hostile actions in the intermission. On the other hand, a civilian who has joined a military organization and commits a chain of hostile acts, with short periods of rest between them, loses his immunity

110 Interpretive Guidance, above note 14, p. 73.
111 *Ibid.*, pp. 70–71.
112 Israel High Court of Justice, *Targeted Killings*, above note 88, para. 40.
113 Interpretive Guidance, above note 14, pp. 70–71.
114 See the description of direct participation in hostilities as potentially "intermittent and discontinuous" in ICTR, *The Prosecutor v. Strugar*, Case No. IT-01-42-A, Judgment (Appeals Chamber), 17 July 2008, para. 178.
115 Supreme Court of Israel, *Public Committee against Torture in Israel v. Government of Israel*, Case No. HCJ 769/02, 13 December 2006, para. 39.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

from attack for the entire time of his activity. For such a person, the rest between hostile acts is nothing more than preparation for the next hostile act.[116]

In conclusion, in interpreting direct participation in hostilities, the threshold of harm requires objective likelihood instead of mere subjective intention, and the belligerent nexus must be confirmed while the causal link should be proximate. The temporal scope is of great importance, but is quite tricky to establish. So far, absent international jurisprudence on the matter, clarification of the concept is still left for academic scholarship, future State practice and judicial decisions.

The principle of distinction concerning non-human targets in cyber warfare

All non-human targets[117] can be divided into two categories: military objectives and civilian objects. Civilian objects are all objects which are not military objectives.[118] Only military objectives can be the object of attacks.[119] This part will discuss what can be attacked under the law by applying the principle of distinction in the cyber domain – that is, what constitutes a military objective in the cyber context. It is worrying that almost everything in cyberspace has huge military potential, and the issue of dual-use objects plays a more important role in targeting than ever. With the increasing importance of data in a cyber armed conflict, the question of whether data itself could be regarded as a military objective will also be addressed.

The notion of "military objective": Two equivalent elements

The widely accepted definition of all non-human military objectives is as follows: 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.[120]

The notion of "military objective" is critical since it directly determines what can or cannot be attacked pursuant to the principle of distinction. In reality, the term "military objective" has been interpreted in vastly different ways. Some hold that it means war-fighting or war-sustaining capability for military action in the definition of Article 52(2) of AP I and includes targets that "indirectly but

116 *Ibid.*, para. 39; Daniel Statman, "Targeted Killing", *Theoretical Inquiries in Law*, Vol. 5, No. 1, 2004, pp. 179, 195.

117 The present authors try not to use the term "objects" here because the question about whether there are non-human targets which are not "objects" will be discussed in the following paragraphs.

118 AP I, Art. 52(1); ICRC Customary Law Study, above note 12, Rule 9, pp. 31–32.

119 AP I, Art. 52(2); ICRC Customary Law Study, above note 12, Rule 7, pp. 24–28.

120 AP I, Art 52(2); ICRC Customary Law Study, above note 12, Rule 8, pp. 29–32; Jacob Kellenberger, "International Humanitarian Law at the Beginning of the 21st Century", statement given at the 26th Round Table on Current Problems in International Humanitarian Law, Sanremo, 5–7 September 2002.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

effectively support and sustain the enemy's war-fighting capability".[121] In practical terms, compliance with the first criterion of "effective contribution" will generally result in the advantage required in the second criterion of "definitive military advantage".[122] Others argue that only when these two elements are cumulatively present is there a military objective in the sense of the Protocol.[123] In other words, the test for the military status of an object is twofold and the two requirements are equivalent.[124]

The present authors disagree with the view that "effective contribution" includes targets that "indirectly but effectively support and sustain the enemy's war-fighting capability", especially in the cyber domain. This interpretation is far too broad and defeats the philosophy behind the limitation of military objectives – indeed, by characterizing the contribution as "effective" and the advantage as "definite", the drafters of AP I tried to avoid such a wide-ranging interpretation of what constitutes a military objective.[125] And the broad interpretation would make the distinction even more confusing in the context of cyber warfare;[126] given that almost everything has a military potential in cyberspace, if indirect support could count as effective contribution, the interpretation would become nearly unlimited since it would allow "any of the adversary's information functions that have a bearing on his capability to fight to qualify as a legitimate target".[127] It is therefore at odds with the object and purpose of Article 52(2) of AP I.

Thus, the definition of military objective should contain two equally important elements: effective contribution and definite advantage. The fulfilment of the former element does not automatically lead to the fulfilment of the latter, since these two elements are independent. The definite advantage element was discussed at length when AP I was drafted. The adjectives considered and rejected included the words "distinct" (*distinct*), "direct" (*direct*), "clear" (*net*), "immediate" (*immediat*), "obvious" (*evident*), "specific" (*specifique*) and "substantial" (*substantiel*).[128] It is clear that the word "definite" has its own value and should not be ignored – the advantage has to be definite and concrete.[129]

121 DoD, above note 41, p. 210; Charles J. Dunlap, "The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era", *Strategic Review*, Vol. 9, 2000, p. 17; US Department of the Navy and Department of Homeland Security, *The Commander's Handbook on the Law of Naval Operations*, July 2007, para. 8.2. There are also some opposite views, such as Laurent Gisel, "The Relevance of Revenue-Generating Objects in Relation to The Notion of Military Objective", in ICRC, *The Additional Protocols at 40: Achievements and Challenges*, 18th Bruges Colloquium, 19–20 October 2017.

122 Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, MA, 2010, p. 49.

123 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on APs), para. 2018.

124 E. Mavropoulou, above note 51, p. 44.

125 Marco Sassòli, "Military Objectives", in *Max Planck Encyclopedia of Public International Law*, 2015, para. 7.

126 J. Kelsey, above note 33, p. 1440.

127 M. Roscini, above note 65, p. 186.

128 ICRC Commentary on APs, above note 123, para. 2019.

129 Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts*, Hart Publishing, Oxford, 2008, pp. 60, 131.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

Potential and indeterminate forms of advantage are not acceptable; neither are political ones.[130] In other words, it is prohibited to launch an attack which only offers potential or indeterminate advantages.[131]

These two elements, effective contribution and definite military advantage, are also equivalent. It is often difficult to identify the military advantage anticipated for a given attack, especially in the cyber context, where measuring the effects of a cyber operation can be challenging.[132] In the cyber domain, where the military uses the same cyber infrastructure as the civilian population for its military activity, the second requirement of the definition becomes even more inclusive and one should be cautious with a sweeping conclusion that seriously underestimates the importance of the second element.[133] Cyberspace is relatively resilient compared to other targets. In the case of an attack against a cyber infrastructure like a communication network, the data flow is so flexible that even if certain communication paths are destroyed by the cyber attack, the data packages will have various other possible paths to follow so as to reach their intended destination.[134] In this case, the partial destruction of the network might effectively contribute to military action but will hardly offer a definite advantage in the end. Thus the judgment on a definite military advantage is complex and cannot be automatically satisfied once the effective contribution element is fulfilled.

Definite military advantage in the cyber context is always hard, if not impossible, to measure and quantify. After the Stuxnet incident, while Iran denied that the incident had caused significant damage, the International Atomic Energy Agency reported that Iran had stopped feeding uranium into thousands of centrifuges at Natanz. No one knows what consequences were caused by Stuxnet on the Iranian nuclear programme, and it is still unclear whether the decision to stop using the Natanz centrifuges was due to Stuxnet or to technical malfunctions inherent to the equipment.[135]

What is particularly worth mentioning in the context of cyberspace is that the requirement to identify a definite military advantage associated with attacking a particular target arises most often with respect to potential dual-use objects. A facility can either support solely civil or solely military purposes, but it can also support both purposes simultaneously, making it a dual-use object.[136] Essential infrastructure such as bridges, electricity-generating installations and oil-refining

130 ICRC Commentary on APs, above note 123, para. 2024.
131 *Ibid.*, paras 2024–2025.
132 M. Roscini, above note 65, p. 188.
133 R. Geiss and H. Lahmann, above note 34, p. 388.
134 *Ibid.*
135 Marco Roscini, "Military Objectives in Cyber Warfare", in Mariarosaria Taddeo and Luciano Floridi (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence of Excellence Initiative*, Springer, Cham, 2017, p. 108; Katharina Ziolkowski, *Stuxnet – Legal Considerations*, CCD COE, Tallinn, 2012, p. 5, available at: https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.
136 Dominik Steiger, "Civilian Objects", in *Max Planck Encyclopedia of Public International Law*, 2011, para. 12.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

facilities may also have the potential to serve civil and military purposes at the same time.[137]

The fundamental difference in cyber warfare lies in the *sui generis* nature of cyberspace – namely, the "systemic inter-connectivity of civilian and military infrastructure".[138] For example, it is estimated that approximately 98% of US government communications[139] use civilian-owned and civilian-operated networks.[140] Civilian satellites, routers, cables, servers and even computers are all potential dual-use cyber facilities. The reality is that "every component of the cyber infrastructure, every bit of memory capacity has a military potential", and this blurs the line between civilian objects and military objectives.[141] One Chinese professor, Zhu Lixin of Air Force Engineering University, pointed out that the US military attaches great importance to building resilient intelligence, reconnaissance and surveillance (ISR) systems supported by artificial intelligence and quantum computing, and actively procures weapons such as smart small-diameter bombs, unmanned swarm systems, hypersonic weapons and directed-energy weapons to ensure lethality. So-called ISR systems require expensive machines such as quantum computers, satellites and artificial intelligence systems, many of which serve both military and civilian purposes.[142] Despite all the challenges, for the law, dual-use objects are not a separate category; they must equally fulfil the two-pronged test of Article 52(2) of AP I. The idea that the Internet itself could constitute a military objective is probably untenable, because the use of military code through the Internet might make some military contribution, but it is hardly effective, and it would not justify an attack because the mere disruption of its operations would be highly unlikely to offer the necessary "definite military advantage".[143] In any event, an attack on the whole Internet would breach the principle of proportionality,[144] ergo it would by no means be legal.

Furthermore, as the dual-use concept is not an innovation of cyber warfare, AP I provides a remarkable assumption for *lex scripta*: in case of doubt regarding the object's military status, it shall be presumed not to be so used.[145] Rule 102 of the Tallinn Manual 2.0 also provides that "[i]In case of doubt as to whether an object and associated cyber infrastructure that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so being used may only be made following a careful assessment".[146]

137 *Ibid*.
138 R. Geiss and H. Lahmann, above note 34, p. 385.
139 To avoid ambiguity, in terms of the numbers noted, we would like to remind readers that not all government communication is equal to military communication or military objectives.
140 Eric Talbot Jensen, "Cyber Warfare and Precautions against the Effects of Attacks", *Texas Law Review*, Vol. 88, No. 7, 2010, pp. 1522, 1542.
141 R. Geiss and H. Lahmann, above note 34, p. 388.
142 L. Zhu, "Competition for International Rules in Cyberspace", above note 2, p. 40.
143 International Criminal Tribunal for the former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, 13 June 2000, para. 75.
144 AP I, Arts 51(5)(b), 57(2)(iii).
145 *Ibid.*, Art. 52(3).

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

Whether data falls within the ambit of military objectives

Data has become a cornerstone of life in many societies. During an armed conflict, the manipulation of data to cause physical harm undoubtedly requires the restraint of IHL, but the question of whether the data *per se* may constitute a military objective is also controversial. Cyber attacks are capable of being directed at data without causing physical effects, such as those targeting civilian financial systems. There are some views which hold that only a material, tangible thing can be a military objective in order to qualify as a legitimate target for attacks.[147] In the Tallinn Manual 2.0, only a minority of experts considered that certain data should be regarded as objects, thus constituting a military objective.[148] It is important to illustrate the relationship between the term "military objective" and the term "object". In a nutshell, from the wording of Article 52(2) of AP I – "in so far as *objects* are concerned, *military objectives* are limited to those *objects* which …" – a military objective is an object that meets certain criteria. The disputed point here is whether data *per se* could constitute an object. There are two main reasons to doubt that data could constitute a military objective, and both of them are related to the notion of "object". First, the intangible character of data fails to fit in the ordinary meaning of "object". Second, the ICRC Commentary on the Additional Protocols observes that "an object is characterized … as something visible and tangible".[149] Thus, data obviously does not qualify. Some scholars argue that data should be treated as objects.[150] Their argument is that cyber operations against civilian data are, on a factual level, illegal attacks on civilian targets. It is important to emphasize, in the view of these scholars, that any impact, direct or indirect, on civilian data in actions directed against lawful cyber targets must be measured in the principle of proportionality analysis and subject to the requirement to seek to minimize civilian collateral damage.[151] The advantage of this interpretation is that it protects civilian populations from the potential negative effects of cyber operations, but it is too broad, too inclusive, and would even include cyber operations, such as psychological operations, in which some countries are already engaged in practice on a regular basis.[152] In short, these criticisms and doubts

146 Tallinn Manual 2.0, above note 31, p. 448.

147 Yoram Dinstein, "Legitimate Military Objectives under the Current *Jus in Bello*", *International Law Studies*, Vol. 78, 2002, p. 142.

148 Tallinn Manual 2.0, above note 31, Rule 100, p. 437; M. N. Schmitt, above note 30, p. 269; Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", *International Review of the Red Cross*, Vol. 96, No. 893, 2015, p. 200.

149 ICRC Commentary on APs, above note 123, paras 2007, 2008.

150 See, for example, 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; ICRC Cyber Operations Paper, above note 32, p. 8; ICRC Challenges Report 2015, above note 32, pp. 41–42; ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, Geneva, 2019 (ICRC Challenges Report 2019), p. 28.

151 Michael N. Schmitt, "International Cyber Norms: Reflections on the Path Ahead", *Netherlands Military Law Review*, 17 September 2018, available at: http://puc.overheid.nl/doc/PUC_248171_11;

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

about the position held by most experts on the Tallinn Manual 2.0 focus on the exclusion of data from the protection provided by the law of targeting in AP I. According to this view, even cyber operations without physical consequences should at least be tested by the principle of proportionality and precaution[153] as long as they involve damage to or destruction of data, even if they may only have a potential impact on the civilian population.[154] Other scholars disagree and suggest that data should be regarded as a military objective once it fits the criteria. For those scholars, interpreting data as an object would "greatly expand the class of permissible targets in warfare",[155] and is counter to the object and purpose of enhancing the protection of civilians during situations of armed conflict. Furthermore, the interpretation of the ordinary meaning of "object" is debatable. There are translation discrepancies in the six authentic languages of AP I,[156] including French and Spanish, in which the term "*un bien*" may be translated into English as "a good" or "a property", and in French the legal term includes both tangible and intangible property.[157] As a matter of fact, in the Chinese context, the term "object"[158] generally refers to those items composed of materials that occupy a certain amount of space,[159] and thus intangible data does not count.

Some scholars also hold the opinion that data should be divided into two categories: "operational-level" data and "content-level" data.[160] According to that view, content-level data, such as the text of this article or the contents of medical databases, library catalogues and the like, are largely excluded from the ambit of military objective.[161] Operational-level data, the type of data that gives hardware

152 *Ibid.*; Michael N. Schmitt, "Notion of Objects during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision", *Israel Law Review*, Vol. 48, No. 1, 2015.

153 As noted in Y. Dinstein, above note 46, pp. 164–174, the principle of precaution includes both active precautions in attack (AP I, Art. 57) and passive precaution (AP I, Art. 58). Active precautions in attack mandate "(a) [d]oing everything feasible to verify that the targets to be attacked are lawful [and] (b) [t]aking all feasible precautions in the choice of means and methods of attack, with a view to avoiding – or, at least, minimizing – collateral damage to civilians and civilian objects". Passive precaution requires belligerent parties, "'to the maximum extent feasible', (i) to endeavour to remove civilians and civilian objects under their control from the vicinity of military objectives; (ii) to avoid locating military objectives within or near densely populated areas; and (iii) otherwise to protect civilians and civilian objects against the dangers resulting from military operations".

154 Paul Ducheine and Terry Gill, "From Cyber Operations to Effects: Some Targeting Issues", *Netherlands Military Law Review*, 17 September 2018, available at: https://puc.overheid.nl/doc/PUC_248377_11/1.

155 K. Mačák, above note 150.

156 AP I, Art. 102: "The original of this Protocol, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic, …".

157 K. Mačák, above note 150.

158 The Chinese version of AP I uses the term "物体". See www.icrc.org/zh/doc/assets/files/other/mt_070116_prot1_c.pdf.

159 "由物质构成的, 占有一定空间的个体". See 当代汉语词典, 上海辞书出版社, 2001 (*Contemporary Chinese Dictionary*, Shanghai Dictionary Publishing House, 2001); 现代汉语大词典, 下册, 上海辞书出版社, 2009 (*Modern Chinese Dictionary*, Vol. 2, Shanghai Dictionary Publishing House, 2009);新华汉语词典, 崇文书局, 2006 (*Xinhua Chinese Dictionary*, Chongwen Publishing House, 2006); 近现代词源, 上海辞书出版社, 2010 (*Etymology of Modern Times*, Shanghai Dictionary Publishing House, 2010).

160 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.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

its functionality and ability to perform the tasks required of it, would be considered a military objective.[162]

Regrettably, the question of whether civilian data should be considered as civilian objects and therefore be protected under IHL seems to have received little attention from Chinese scholars. Zhu Yanxin, an associate professor from the Political College of the PLA National Defence University, holds the view that data could be defined as a military objective while not being an object.[163] He argues that data is a "non-object" military objective.[164] This argument is based on the language at the beginning of the second sentence of Article 52 of AP I:

> Attacks shall be limited strictly to military objectives. In so far as *objects* are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[165]

The literal wording of the provision clearly permits the existence of military objectives which are objects and non-objects.

The present authors' views on this point are basically in line with the ICRC's position paper of 2019.[166] Certain data, at least essential civilian data,[167] should fall within the ambit of civilian objects since the ordinary meaning of "object" is evolving and it would suit the object and purpose of the Geneva Conventions and their Additional Protocols. The term "object" does not necessarily exclude data from the scope of military objectives; we must bear in mind that the ordinary meaning of "object" should not be limited to that of the time when the treaty was adopted, and will evolve over time.[168] A treaty interpretation based solely on a textual approach ignores other methods of interpretation enshrined in the Vienna Convention on the Law of Treaties.[169] For instance, from the perspective of the object and purpose of AP I, the idea that "deleting or tampering with essential civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL".[170] It is a convincing argument to state that the replacement of paper files and documents with digital files in the form of data should not

161 *Ibid.*
162 *Ibid.*
163 朱雁新, 数据的性质: 对军事目标法律含义的重新解读, 载黄志雄主编, 网络空间国际规则新动向: "塔林手册2.0版" 研究文集, 社会科学文献出版社, 2019: 410–413 (Yanxin Zhu, "The Nature of Data: A Reinterpretation of the Legal Meaning of Military Objective", in Zhixiong Huang (ed.), *New Trends in International Rules for Cyberspace: Collection of Papers on Tallinn Manual 2.0*, Social Sciences Academic Press, China, 2019, pp. 410–413, only available in Chinese).
164 *Ibid*, p. 410.
165 AP I, Art. 52(2).
166 ICRC Cyber Operations Paper, above note 32, p. 8.
167 *Ibid.*, p. 8.
168 K. Mačák, above note 150.
169 See Vienna Convention on the Law of Treaties, 1155 UNTS 331, 23 May 1969 (entered into force 27 January 1980), Art. 31(3)(a).
170 ICRC Cyber Operations Paper, above note 32, p. 8.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

decrease the protection that IHL affords to them.[171] If data is not an object, cyber operations against civilian data become a vacuum in IHL, and cyber operations that cause substantial damage to civilian life are not prohibited by law.[172]

The Tallinn Manual 2.0 equates military objectives with objects. To illustrate, the definition of military objectives proposed in Rule 100 leaves no space for non-objects: "Military objectives are those objects which …".[173] The viewpoint that data could constitute a military objective while not being an object is questionable for two main reasons. Firstly, this idea would shake the traditional persons–objects dichotomy, which, insofar as the construction of these provisions is concerned, appears to be correct; States have even rejected a third category such as "places".[174] Secondly, it would consequently leave no valid criterion for assessing whether a specific data set would be a military objective.[175] The persons–objects dichotomy provides the criteria of effective contribution and definite advantage for non-living things, while there are other requirements for living targets.[176] If data is not an object, this would lead to the unreasonable position that data needs to be assessed on the same basis as living targets. Therefore, the idea that data could be defined as a military objective while not being an object is not persuasive.

Conclusion

Cicero's aphorism, "during war, the laws are silent" (*silent enim legis inter arma*), does not reflect the modern reality. Despite all the challenges involved, the *jus in bello* principle of distinction is applicable to cyber warfare. Because of the lack of treaty provisions and judicial decisions specific to the cyber realm, the interpretation of existing law is based on the available academic discussion and limited State practice. There is a need for general clarification and further development of the principle of distinction in the cyber context; for example, the definitions of "cyber military objective" and "cyber combatant" remain controversial. Just as the UN Secretary-General mentioned at the World Economic Forum, "we need to find a minimum of consensus in the world on how to integrate these new technologies in the laws of war that were defined decades ago in a completely different context".[177]

Up to now, the Chinese government has not been clear about the application of IHL in cyberspace. There are indeed Chinese academic papers that look at the application of IHL in cyberspace, but the discussion of the principle of

171 ICRC Challenges Report 2019, above note 150, p. 28.
172 See M. N. Schmitt, above note 151.
173 Tallinn Manual 2.0, above note 31, p. 435.
174 M. Bothe, K. J. Partsch and W. A. Solf, above note 87, pp. 301–304.
175 K. Mačák, above note 150.
176 AP I, Art. 52(2).
177 World Economic Forum, "António Guterres: Read the UN Secretary-General's Davos Speech in Full", 24 January 2019, available at: www.weforum.org/agenda/2019/01/these-are-the-global-priorities-and-risks-for-the-future-according-to-antonio-guterres/.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

distinction in cyberspace is limited both in length and in academic depth. Compared with the West, the research of Chinese scholars on this issue is still in a relatively preliminary stage. At present, there is no specific deconstruction or clarification of the application of the principle of distinction in cyberspace in Chinese academia.

Despite the potential technical challenges and uncertainties involved, the principle of distinction should be applied to cyberspace. It should also be carefully re-examined and clarified from the standpoint of preventing over-militarization and maximizing the protection of the interests of civilians. For human targets, the elements identified in customary international law and relevant IHL treaties to determine who is a combatant are not well suited to the digital battlefield. Nevertheless, cyber combatants are still obligated to distinguish themselves from civilians. In applying the principle of distinction, the present authors argue that it makes more sense to focus on substantive elements rather than formal elements such as carrying arms openly or having a fixed distinctive sign recognizable at a distance. In interpreting "direct participation in hostilities", the threshold of harm requires an objective likelihood instead of mere subjective intention, and the belligerent nexus should be confirmed while the causal link should be at least proximate. Applying the "cyber kill chain" model by analogy helps us to grasp the whole process of direct participation in hostilities during cyber warfare. For non-human targets, all military objectives must cumulatively fulfil both the effective contribution and definite military advantage criteria, which are equally indispensable. The same requirements apply to dual-use objects. As for the status of data, the ordinary meaning of "object" is debatable. There are translation discrepancies in the six authentic languages of AP I; in French the legal term includes both tangible and intangible property, while under the Chinese context, the term generally refers to those items composed of materials that occupy a certain amount of space, and thus intangible data does not count. Furthermore, one Chinese scholar argues that certain data belongs in the category of "non-object" military objective.

With the popularization of internet technology, unprecedented changes have taken place in the twenty-first century. The future of IHL in cyberspace still lies in the hands of States, particularly as they interpret the extant provisions and norms. War, technology and the *jus in bello* have been substantively intertwined and have interacted with each other since the beginning of organized human conflict, but the law has been constantly forced to adjust and is seemingly always "one war behind reality".[178] Therefore, faced with changes in technology and science, it is preferable to use methods of dynamic and evolving interpretation of international treaties and principles of international law in order to give them their full effect. It must be recognized that the increasing evolution of weapons and the rapid development of science and technology will have a tremendous

178 Jimena M. Conde Jiminián, "The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law", *Tilburg Law Review*, Vol. 15, No. 1, 2010. See also Marco Sassòli, Antoine Bouvier and Anne Quintin, *How Does Law Protect in War?*, 3rd ed., Vol. 1, ICRC, Geneva, 2011, p. 52.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press

impact on human society and that the *jus in bello* will adjust and adapt accordingly. However, it would be naive to assume that changes to IHL will be timely and effective.

It is probably too early to advocate for the adoption of a new treaty in this area. In any event, the prospects that States will agree on a comprehensive convention on cyber warfare in the near future are quite slim. Instead, the existing *lex lata* provides the basic regulation on targeting in the cyber domain. State practice, judicial decisions and scholars' views and teachings should take the lead on the interpretation of the existing legal framework and the assessment of whether the humanitarian concerns served by it are satisfied or undermined in the interconnected domain of cyberspace. Predictably, in the course of this evolution, States may try to analogically reason, induce or creatively fill in the gaps of the existing IHL, or push the *lex lata* concerning the principle of distinction beyond its normative boundaries when implementing new strategies in the era of cyber warfare. This trend needs to be strictly limited; however, it would be arbitrary to exclude the possibility of setting new rules. From the standpoint of preventing over-militarization and maximizing the protection of the interests of civilians, it is necessary to re-read the principle with great caution. While there have admittedly been no mass-casualty cyber events so far, when the interpretation and clarification of the existing rules are not enough, new rules need to be proposed before a "cyber Pearl Harbor" incident occurs.[179]

179 DoD, above note 4; J. J. Wirtz, "The Cyber Pearl Harbor", above note 4; J. J. Wirtz, "The Cyber Pearl Harbor Redux", above note 4.

https://doi.org/10.1017/S1816383121000023 Published online by Cambridge University Press