One Click from Conflict: Some Legal Considerations Related to Technology Companies Providing Digital Services in Situations of Armed Conflict

Jonathan Horowitz*

Abstract

Private technology companies (tech companies) are increasingly providing their digital goods and services to clients living and working in situations of armed conflict. Tech companies may own, operate, or maintain significant portions of the digital infrastructure that allow day-to-day essentials—such as water, medical care, and electricity—to reach civilians living in places affected by armed conflict. They may own communications platforms that people use to call emergency services. They may own social media outlets that organizations rely on to inform communities in need about access to humanitarian services or that families use to maintain contact with each other. Those fighting today's armed conflicts, including well-resourced militaries, and less-developed non-state armed groups, also undoubtedly rely on hardware, software, and networks manufactured, serviced, and secured by tech companies. They use them to coordinate and carry out a wide array of military operations, including the management of troop movements, military fuel and spare parts, and medical supplies. This paper's premise is that as tech companies increase their involvement in armed conflict, the legal implications they face under international humanitarian law (IHL)—a body of law that regulates who and what is protected from the hostilities of armed conflict—also rise. Recognizing that cyberspace spans the globe with little concern for geography and borders, Section II discusses how this reality effects the applicability of IHL's principles and rules relating to tech company employees and properties. From there, Section II explains the protections IHL affords the employees and properties of tech companies operating in situations of armed conflict and when, in exceptional circumstance, those protections might be lost. Section III moves on to discuss how IHL addresses situations where civilians and civilian objects get caught in the "digital crossfire" when they are reliant on, or located in proximity to,

---

* Legal Adviser at the International Committee of the Red Cross (ICRC). I would like to thank Samit D'Cunha, Pierrick Devidal, Laurent Gisel, Duncan Hollis, Victoria Luckenbaugh, Kubo Mačák, Ralph Mamiya, Laura Walker McDonald, Matt Pollard, Tilman Rodenhäuser, Fasya Addina Teixeira, Mauro Vignati, Lakmini Seneviratne, Austin Shangraw, Mark Silverman, and Claude Voillat for their comments on earlier drafts. This article was written in a personal capacity and does not necessarily reflect the views of the ICRC.

tech companies involved in armed conflict. Section IV concludes with practical recommendations for companies to take to minimize risks to their employees, property, civilian customers and surrounding civilians and civilian objects, including civilian infrastructure.

Table of Contents

I. INTRODUCTION

Private technology companies (tech companies) are increasingly providing their digital goods and services to clients living and working in situations of armed conflict. These companies may own, operate, or maintain significant portions of the digital infrastructure that allow day-to-day essentials—such as water, medical care, and electricity—to reach civilians living in places affected by armed conflict. Information and telecommunications companies may provide people with the ability to call emergency services. Social media companies may own platforms that organizations rely on to inform communities in need about access to humanitarian services or that families use to maintain contact with each other. Those fighting today's armed conflicts, including well-resourced militaries and less-developed non-state armed groups, also undoubtedly rely on hardware, software, and networks manufactured, serviced, and secured by digital tech companies. Cloud computing and other digital services offer opportunities for belligerents to coordinate and carry out a wide array of military activities, including the management of troop movements, military fuel and spare parts, and medical supplies. As this paper discusses, some of these military activities might make some of this digital infrastructure lawfully targetable under international humanitarian law (IHL), but some of these activities, such as medical services, would be protected from attack.[1]

The urbanization of warfare—the phenomenon of parties increasingly fighting in urban areas where civilians bear the brunt of the hostilities—is another factor pulling the tech sector into armed conflicts due to the interconnected presence and density of the sector's hardware, software, network infrastructure, and services.[2] Additionally, many States are, in times of peace, developing national cyber security strategies reliant on a backbone built of private-public partnerships that will presumably carryover into times of war.[3] Through these or other close

---

1 Dr. Cordula Droege, *Keeping Civilians Off-Limits in Present and Future Wars*, DIGITAL FRONT LINES, https://perma.cc/E49B-82LB ("The ability and agility of tech companies to respond to cyber operations have been praised, but what unintended consequences arise when they defend infrastructure against military operations or provide cloud storage and communication infrastructure to belligerents? Using civilian infrastructure and services for military purposes exposes them to cyber and kinetic attacks.").

2 For more on the phenomenon of urbanization of warfare, *see* International Committee of the Red Cross (ICRC), INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 16–19 (Geneva, 2019), https://perma.cc/VZL3-SK7D.

3 In the United States, for example, in August 2021, Amazon, Google, and Microsoft became some of the headlining names to take part in a collaborative initiative between the U.S. government and private industry to boost U.S. cybersecurity. *See* Press Release, Cybersecurity and Infrastructure Security Agency, CISA Launches New Joint Cyber Defense Collaborative (Aug. 6, 2021), https://perma.cc/3VAS-W9DR; Dan Reilly, *Cybersecurity Experts Say Public-Private Partnership is the Key to Preventing Future Attacks*, FORTUNE (Nov. 16, 2021), https://perma.cc/A8SE-W755.

partnerships, tech companies may find themselves—whether voluntarily or out of a legal obligation—working with States that are parties to an armed conflict.

Also consider that unwitting civilians risk being exposed to harm when, for example, one side of an armed conflict targets a company's products or services that both civilians and the adversary rely on. Given the ubiquity of digital services in our daily lives, cyberspace's interconnected uses by civilians and militaries expose civilian populations to the harms of "digital crossfire," including harms that IHL—a body of law that regulates who and what is protected from the hostilities of warring parties—aims to avoid or minimize but may not entirely prohibit.

This paper's premise is that as tech companies increase their involvement in armed conflict, the legal implications they face under IHL also rise. Recognizing that cyberspace spans the globe with little concern for geography and borders, Section II discusses how this reality affects the applicability of IHL's principles and rules relating to tech company employees and properties. From there, the section explains the protections IHL affords to the employees and properties of tech companies operating in situations of armed conflict and when, in exceptional circumstances, those protections might be lost. Section III moves on to discuss how IHL addresses situations where civilians and civilian objects get caught in the "digital crossfire" when they are reliant on, or located in proximity to, tech companies involved in armed conflict.

While parties to an armed conflict are the ones primarily responsible for complying with IHL, Section IV concludes with practical recommendations for

---

Consider also the 2018 Paris Call for Trust and Security in Cyberspace, which sought to organize "all cyberspace actors," including States and the private sector, around nine principles, the first of which was to "prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure." The Paris Call—with 81 States, 706 companies and private sector entities, and many other supporters as of December 1, 2023—was primarily focused on responding to cyber insecurity during times of peace. But its approach holds the potential to draw these companies into armed conflicts as the information and communications technology (ICT) environment becomes an increasingly common space where military operations take place. *See* PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE, https://perma.cc/V2WK-TW36. Additionally, in the wake of the international armed conflict between Russia and Ukraine, Microsoft (a supporter of the Paris Call) observed that "the role the private sector now plays in protecting a country in a time of war" is new to the armed conflict landscape in the 21st century and that this "imposes a heightened responsibility on tech companies to use the best technology available and sometimes to take extraordinary measures to help defend a country from attack." *See* MICROSOFT, DEFENDING UKRAINE: EARLY LESSONS FROM THE CYBER WAR 7 (June 22, 2022), https://perma.cc/LP9M-BFAF. Google, also a supporter of the Paris Call, said in the context of the international armed conflict between Russia and Ukraine that it provides services to help "the Ukrainian government detect, mitigate, and defend against cyber attacks." *See* GOOGLE, FOG OF WAR: HOW THE UKRAINE CONFLICT TRANSFORMED THE CYBER THREAT LANDSCAPE 2 (Feb. 2023), https://perma.cc/5L93-GEYJ. Not all companies may agree with Microsoft or Google's approach, but it provides an illustration of how two (large) companies positioned themselves.

companies to take to minimize risks to their employees, property, and surrounding civilians and civilian objects, including civilian infrastructure. These recommendations build off of the United Nations Guiding Principles on Business and Human Rights[4] as well as the United Nations mandated Working Group on Business and Human Rights, which places an emphasis on companies adopting conflict sensitive approaches and heightened due diligence to identify, prevent, mitigate, and account for how businesses address their adverse impacts.[5]

With its focus on IHL, this paper does not address situations where tech companies are providing digital services outside the context of an armed conflict, including activities that are unrelated to an armed conflict even when they occur in the territory where an armed conflict is taking place. Conclusions drawn from this paper therefore are not applicable to the provision of digital service that are not linked to an armed conflict.[6]

II. PRIVATE TECHNOLOGY COMPANIES UNDER IHL

A. Applicability of IHL and Geographic Considerations

International humanitarian law is a body of international law that applies to, and only to, situations of "armed conflict," which is a legal term with precise legal definitions.[7] More specifically, IHL regulates the behavior of parties to armed

---

4 H.R.C. Res. 17/31 (Mar. 21, 2011), endorsed by the Human Rights Commission in H.R.C. Res. 17/4 (July 6, 2011).

5 *See* United Nations Development Programme, Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide (2022), https://perma.cc/SQT7-QCJG. The recommendations also take into account the important work of a high-level multidisciplinary group of experts that examined digital threats during armed conflict. *See* ICRC, PROTECTING CIVILIANS AGAINST DIGITAL THREATS DURING ARMED CONFLICT: RECOMMENDATIONS TO STATES, BELLIGERENTS, TECH COMPANIES, AND HUMANITARIAN ORGANIZATIONS (2023) FINAL REPORT OF THE ICRC GLOBAL ADVISORY BOARD ON DIGITAL THREATS DURING ARMED CONFLICT, https://perma.cc/CG6N-BXTM.

6 *See* ICRC, THE USE OF FORCE IN ARMED CONFLICTS: INTERPLAY BETWEEN THE CONDUCT OF HOSTILITIES AND LAW ENFORCEMENT PARADIGMS 5 (Gloria Gaggioli ed., ICRC, 2013), https://perma.cc/97CP-5JTA ("In order to be covered by IHL, the use of force must take place in an armed conflict situation and must have a nexus with the armed conflict."); TALLINN MANUAL 2.0 ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS Rule 80 ¶ 5 (Michael N. Schmitt and Liis Vihul eds., Cambridge Univ. Press, Cambridge, 2d ed. 2017) ("There must be a nexus between the cyber activity in question and the conflict for the law of armed conflict [i.e., IHL] to apply to that activity."), https://perma.cc/7RAM-T9NG.

7 *See* Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INT'L REV. RED CROSS 69, 69–94 (2009), https://perma.cc/J2XC-SJ2X.

For exceptions to the rule that IHL applies only in situations of armed conflict, *see* Kubo Mačák, *Unblurring the Lines: Military Cyber Operations and International Law*, 6:3 J. CYBER POL'Y 411, 417–418 n. 2 (2021) ("These exceptions relate primarily to measures that must be taken in peacetime in order to ensure the respect for IHL in the event an armed conflict occurs, such as the duties to disseminate

conflict by placing limits on their means and methods of warfare and by providing various protections to the civilian population and others. The limits and protections reflect a balance between the principles of humanity and military necessity, with the object and purpose of IHL being to limit the suffering caused by war and to alleviate its effects.[8] This balance shapes the context in which IHL's rules and other principles (such as distinction, proportionality, and precautions) must be interpreted.[9] Each of these principles are elaborated on below. But, in summary, the principle of distinction prohibits directing attacks at civilians and civilian objects, and requires limiting attacks only against combatants and military objects, provided the attacks comply with other rules and principles of IHL.[10] The proportionality principle prohibits attacks that are expected to cause civilian harm that is excessive in relation to the concrete and direct military advantage anticipated.[11] And the principle of precaution obligates belligerents to take all feasible precautions to avoid, or at least minimize, incidental civilian harm from attacks.[12] It also obligates parties to do everything feasible to protect civilians and civilian objects under their control from the effects of an adversary's attack.[13]

States, academics, and others have heatedly debated whether IHL applies to belligerents conducting cyber operations in armed conflict. The emerging consensus is that it does. Notably, in 2021, States collectively agreed it was time to start assessing "how" and "when" IHL applies rather than isolate the discussion only to "whether" it applies.[14] There nonetheless remain other important questions around IHL's applicability to consider. Notably for the cyber context, IHL's applicability is often said to extend to the entirety of the territory of the State (or States) where an armed conflict is taking place.[15] This means that IHL's

---

and train IHL, to adopt certain implementing domestic legislation, to carry out legal reviews of new weapons, means and methods of warfare, or to take measures to protect civilians against the effects of attacks.").

8 *See* Cordula Droege and Eirini Giorgou, *How International Humanitarian Law Develops*, 104 INT'L REV. RED CROSS, 1798, 1799 (2022).

9 ICRC, Cyber Operations in Armed Conflict: The Principles of Humanity and Necessity (Mar. 2023), https://perma.cc/JCF8-EHG4.

10 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, VOL. 1: RULES (Jean-Marie Henckaerts and Louise Doswald-Beck eds., Cambridge Univ. Press 2005), at Rules 1 and 7.

11 *Id.* at Rule 14.

12 *Id.* at Rules 15–21.

13 *Id.* at Rules 22–24.

14 Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, ¶ 71(f), U.N. Doc. A/76/135 (July 14, 2021), https://perma.cc/YU4K-XUH6.

15 Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 68 (Int'l Crim. Trib. For the Former Yugoslavia Oct. 2, 1995); Dieter Fleck, *Scope of Application of International Humanitarian Law*, *in* HANDBOOK OF INTERNATIONAL HUMANITARIAN

principles and rules on what is protected from attack would apply to tech company employees and properties located in the territory of such States. While the remaining sections of this paper relate to tech companies operating under these circumstances, cyberspace networks span the globe with little concern for geography and borders. A tech company with employees and property located in the territory of a State *not* party to an armed conflict may therefore be capable of providing goods and services in the territory of a State where an armed conflict exists. This can include providing goods and services in support of the warring parties. In such situations, the question arises whether IHL is the proper body of international law to regulate whether and how those employees and property are protected from being attacked.

This paper does not address this question in detail. Suffice it to say that it will primarily be the *jus ad bellum*—the body of international law regulating the resort to use of force between States—that determines if a State is prohibited or not from taking such action against a tech company located in a non-belligerent State (i.e., a State not party to an armed conflict). Under this body of law, a State is prohibited from using force against another State without its consent.[16] The only exceptions to this rule are if the U.N. Security Council authorizes the use of force or when a State can make a claim to act on its inherent right to self-defense against an "armed attack."[17] Some States debate whether a cyber operation can ever amount to an "armed attack." For those States that agree that it can, they often point out that any action taken in self-defense must be necessary and proportionate.[18]

Debates also exist over whether a State may ever claim a right to self-defense in response to the acts of non-state groups that are unattributable to another State. There is additional controversy over the requisite organizational attributes of such groups and, moreover, whether a single individual could ever engage in acts that could provide a legitimate claim to self-defense.[19] These legal issues are of course directly relevant to the foundational question of *whether* the acts of private tech company employees located in a non-belligerent State could ever make them or the properties of their company potential targets in the name of self-defense.

Whatever the answer is to that legal question, there remain legal and other considerations to take into account. Private individuals, including tech company

---

LAW 65-68 (Dieter Fleck ed., 4th ed. OUP, 2021); Jelena Pejic, *Extraterritorial Targeting by Means of Armed Drones: Some Legal Implications*, 96 INT'L REV. RED CROSS 67, 94–95 (2014).

16 U.N. Charter art. 2, ¶ 4, https://perma.cc/VGX6-5Y5X.

17 *Id.* at arts. 42 and 51. With regard to State views on "armed attacks" and "imminent armed attacks" in the cyber context, *see Self-Defense*, CYBERLAW TOOLKIT, https://perma.cc/R7M4-B9P4.

18 *See Self-Defense,* CYBERLAW TOOLKIT, https://perma.cc/R7M4-B9P4; TALLINN MANUAL 2.0, *supra* note 6, at Rule 72 ("A use of force involving cyber operations undertaken by a State in the exercise of its right of self-defence must be necessary and proportionate.").

19 TALLINN MANUAL 2.0, *id.* at Rule 71 ¶¶ 18–20.

employees, located in a non-belligerent State who support one side of an armed conflict or harm the other side still have the potential to cause significant foreign relations consequences, even if their actions cannot trigger claims of self-defense. These could include undesired and escalatory diplomatic exchanges between States, claims that the hosting State is breaching the law of neutrality for not ceasing a tech company's support to a party to an armed conflict, law enforcement responses such as criminal charges against the employee and extradition requests, and economic sanctions against a company and its employees.

Consider also what happens if—whether lawfully or not under the *jus ad bellum*—a State takes action against a tech company located in a non-belligerent State. If this action constitutes a resort to armed force as understood under IHL, then IHL will become applicable. That standard—"resort to armed force"—is the standard that brings into existence an international armed conflict as defined under Article 2 common to the four 1949 Geneva Conventions and, as such, IHL would then regulate that use of force (and any subsequent hostilities) by virtue of it being part of the new international armed conflict.[20] Under this interpretation, the resort to armed force (whether through kinetic or through another type of operation that would amount to this standard) against a tech company's employees or properties, even if located in a non-belligerent State, would then have to comply with IHL, and in particular with its principles and rules of distinction, proportionality, and precaution.

Having just touched on the topic of IHL, the remainder of this paper explores additional IHL implications that arise when a tech company's employees and properties are located in a State where an armed conflict is taking place.

B. IHL Implications for Tech Companies Operating in Armed Conflicts

A quick internet search of job openings at Amazon, Google, Huawei, Meta, Microsoft, and Yandex illustrates who big tech companies employ.[21] They include

---

20 ICRC, COMMENTARY ON THE THIRD GENEVA CONVENTION: CONVENTION (III) RELATIVE TO THE TREATMENT OF PRISONERS OF WAR ¶¶ 250–52 (2d ed. 2020), https://perma.cc/LD6W-K9HY. For the specific cyber context, *see* ¶¶ 286–89. *See also*, Kubo Mačák, *Scenario 13: Cyber operations as a trigger of the law of armed conflict*, CYBERLAW TOOLKIT, https://perma.cc/PX33-PKZM.

While debates exist over whether a use of armed force directed at a private entity can bring into existence an international armed conflict, the ICRC takes the view that such acts need not be directed against the enemy State's armed forces, but may also be directed at its "territory, its civilian population and/or civilian objects, including (but not limited to) infrastructure." *See* ICRC COMMENTARY ON GC III at ¶ 257.

21 *See Find jobs by job category*, AMAZON, https://perma.cc/9KKB-UKV7; *Google Careers*, GOOGLE, https://perma.cc/C7Y2-GNYX; *Huawei Career*, HUAWEI, https://perma.cc/YPD8-54N8; *Vacancies*, KASPERSKY, https://perma.cc/CS37-X4CG; *Meta Careers*, META, https://perma.cc/SJJ3-CRMD; *Careers: Professions*, MICROSOFT, https://perma.cc/9BEZ-9VGV; *Vacancies*, YANDEX, https://perma.cc/7R95-6HXX.

people who work in hardware and software development, incident response, marketing, retail, security and support services, and many other fields. It would similarly be impossible to provide an exhaustive list of all the types of properties tech companies own and operate. They might include office buildings, production factories, warehouses, and the land their built on; the personal computers, printers, desks, and company delivery trucks used by employees; and company routers, modems, fiber optic cables, and other hardware, software, network infrastructure, and data.

It is helpful to parse out tech companies in this way because many of IHL's most foundational principles and rules relate to people and objects. Most notably, IHL affords civilians and civilian objects protection against direct attack by parties to armed conflict. In contrast, parties to an armed conflict are not prohibited from directing attacks against combatants and military objectives,[22] provided other applicable principles and rules of IHL are complied with.[23] Paired together, these two rules form IHL's cardinal principle of distinction. Whether that protection from attack is afforded to the employees and properties of a private tech company, therefore, generally boils down to assessing whether its employees and any pieces of property qualify as "civilians" and "civilian objects" under IHL, respectively.

1. Company employees and direct participation in hostilities.

Generally, tech company employees qualify as civilians and therefore must not be attacked. That is true because the employees usually are not members of a State's armed forces; their company is not regarded as "belonging to a party to an armed conflict,"[24] and they are not directly participating in hostilities (DPH). If, however, exceptional circumstances arise where an employee falls into any one of these three categories, they may no longer be protected from attack. Tech companies and their employees need to be aware of all three categories, but this paper focuses only on the issue of DPH.

Civilians were never meant to directly participate in hostilities on behalf of a party to an armed conflict.[25] But history has repeatedly shown that they nonetheless do.[26] In response to the untenable result of civilians participating in hostilities while being legally shielded against being attacked, Article 51(3) of

---

22 *See* ICRC, CUSTOMARY LAW STUDY, *supra* note 10. For persons and objects generally *see* Rules 1 and 7. *See* Part II on specifically protected persons and objects.

23 These principles and rules include, in particular, the prohibition against indiscriminate and disproportionate attacks, and the obligations to take precautionary measures. *See id.* at Rules 11–21. For further discussion of these principles and rules, *see* Section III below.

24 Nils Melzer, ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law 69 (2009).

25 *Id.* at 38–39.

26 ICRC, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 15 (2007), https://perma.cc/P7T5-9GLP.

Additional Protocol I, which reflects customary international law applicable in international and non-international armed conflict, codified as treaty law the rule that civilians shall be protected against attack "unless and for such time as they take a direct part in hostilities."[27] The questions then arise: what constitutes direct participation in hostilities, and how is it applied to a civilian tech company employee engaging in activities related to an armed conflict?

In 2003, the International Committee of the Red Cross (ICRC) and T.M.C. Asser Institute initiated a project to help clarify the contours of DPH. The project consisted of expert consultations spanning six years. During that time, the experts discussed countless operational contexts and scenarios, including DPH's relationship to cyberspace. Experts considered, for example, whether civilians should lose their protection against attack when making use of electronic means with the aim of diminishing the military capacity of an adversary (this was specifically in reference to "computer network attacks (CNA)");[28] when electronically seizing control over remotely guided weapons, weapons carriers, or computer networks used by the adversary;[29] when providing, gathering, analyzing, and transmitting intelligence data through unauthorized access to computer networks used by an adversary;[30] and when electronically depriving an adversary access to financial assets or resources by seizing control over bank accounts and cash reserves.[31]

After the consultations concluded, the ICRC published its Interpretive Guidance on the matter in 2009.[32] According to that guidance and as echoed by certain States,[33] determining whether a civilian is engaging in DPH requires applying a precise and purposefully narrow three-part cumulative test.

---

27 Protocol Additional (I) to the Geneva Conventions of Aug. 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, art. 51(3), June 8, 1977 (entered into force Dec. 7, 1978), 1125 U.N.T.S. 3; ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 6.

28 ICRC, DIRECT PARTICIPATION IN HOSTILITIES UNDER IHL EXPERT MEETING (GENEVA, OCT. 25–26, 2004) BACKGROUND DOCUMENT 5, https://perma.cc/SYA8-38AT.

29 *Id.* at 9.

30 *Id.* at 12.

31 *Id.* at 9–10. *See also* ICRC, THIRD EXPERT MEETING ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES (GENEVA, OCT. 23–25, 2005) SUMMARY REPORT 14–15, https://perma.cc/7LHD-HN45.

32 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24.

33 With regard to the cyber context *see e.g.*, Colombia, *Manual de Derecho Operacional (Operational Law Manual)* (2d ed. 2015), Ministerio de Defensa Nacional, Comando General de las Fuerzas Militares, Santafé de Bogotá, 42–43; Denmark, *Military Manual on international law relevant to Danish armed forces in international operations*, Danish Ministry of Defence, Defence Command Denmark, 2016, 168–69; France, *International Law Applied to Operations in Cyberspace*, Ministry of the Armies, 2019, 15; Federal Government of Germany, *On the Application of International Law in Cyberspace*, Position Paper 8 (Mar. 2021). Taking a similar approach, *see* Norway, *Manual I krigens folkerett*, 2013 ¶¶ 3.24–3.27. With

> 1. The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack (known as the "threshold of harm" criterion);
>
> 2. 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 (known as the "direct causation" criterion); and
>
> 3. The act must be specifically designed to directly cause the required threshold of harm in support of a party to the armed conflict and to the detriment of another (known as the "belligerent nexus" criterion).

When all three criteria are cumulatively met, the consequences are significant. Notably, the civilian—who otherwise had unconditional protection from attack—loses that protection for such time as they are engaging in DPH. Another consequence is that when a civilian engages in DPH they expose proximate civilians and civilian objects to risks of incidental harm that IHL aims to avoid or at least minimize but may not fully prohibit.[34]

Given that the object and purpose of IHL is to limit the suffering caused by war and to alleviate its effects, the three DPH criteria were narrowly tailored to reflect, as one expert put it, that "not everything beneficial to the military is DPH."[35] As an illustration, the group of experts who gathered to write the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*) agreed that "designing malware and making it openly available online, even if it may be used by someone involved in the conflict to conduct an attack" does not constitute DPH.[36] The Tallinn experts drew the same conclusion for "maintaining computer equipment generally, even if such equipment is subsequently used in the hostilities."[37] But it is equally true that civilian activities in or through cyberspace may qualify as DPH.

---

regard to the views of experts, *see* TALLINN MANUAL 2.0, *supra* note 6, at Rule 97 ¶ 5 ("The International Group of Experts generally agreed with the three cumulative criteria for qualification of an act as direct participation that are set forth in the ICRC Interpretive Guidance.").

34 For further discussion of this issue, *see* Section III below.

35 Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, *Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*, 102 INT'L REV. RED CROSS 287, 313–14 (2020), https://perma.cc/B48H-7HXW; ICRC, SECOND EXPERT MEETING ON DIRECT PARTICIPATION IN HOSTILITIES UNDER IHL (THE HAGUE, OCT. 25–26, 2004) SUMMARY REPORT 6, https://perma.cc/8FJP-HGQB; Elizabeth Mavropoulou, *Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks*, 4:2 J.L. CYBER WARFARE 23, 87 (2015), https://perma.cc/NU76-8RPA ("All three requirements applied together in conjunction constitute a relatively high threshold for the notion of direct participation in hostilities in the cyber context.").

36 TALLINN MANUAL 2.0, *supra* note 6, at Rule 97 ¶ 6.

37 *Id.*; *see also* K. Mačák, *Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield*, 105 INT'L REV. RED CROSS 965, 973 (2023).

a) Threshold of harm criterion

The first criterion listed in the DPH guidance—the "threshold of harm" criterion—requires that "the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack."[38] Adverse effects on military operations or capacity is not confined to killing or injuring people or damaging objects. It may include, for example, adverse effects on troop movements, logistics, and communications.[39] It is also regularly accepted that the requisite harm may be met through offensive and defensive activities.[40] The DPH Guidance also explained that "[e]lectronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack."[41]

In the cyber context, where proliferation of tools that civilians now have access to and the ease at which they can cause disruptions, the DPH criteria demands scrupulous application. For example, the threshold of harm criterion requires causing a concrete impact on enemy operations or activities. Otherwise, it cannot be said to be "adversely affecting" them.[42]

The fact that the threshold of harm criterion will "generally be satisfied regardless of quantitative gravity," provided it is expected to cause harm "of a specifically *military nature*,"[43] also demands applying narrow interpretations of the other two criterion and the temporal element of the notion of DPH. In other words, for the DPH test to retain its protective value, its other criteria and elements must be restrictively interpreted. Beyond this, it could be advisable for States to clarify whether a specific threshold of harm for adverse military effects

---

38 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 46.

39 *See e.g.,* Norway Manual, *supra* note 33, at ¶ 3.25; Denmark Manual, *supra* note 33, at 169 ("The requirement of adversely affecting the military operations of the adversary does not require the act to result in physical harm or destruction.").

40 *See* N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 48; TALLINN MANUAL 2.0, *supra* note 6, at Rule 92; ICRC, AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS DURING ARMED CONFLICTS: EXPERT MEETING (GENEVA, JAN. 21-22, 2020) REPORT 16–17 (Ewan Lawson and Kubo Mačák eds., ICRC, Geneva, May 2021), https://perma.cc/6TEJ-5T95. *See also*, Denmark Manual, *supra* note 33, at 169 (stating that "[g]uarding and other protection of facilities, persons, or equipment that constitute military objectives when the task entails protection against attack from the armed forces of the adversary" meets the threshold of harm criteria.).

41 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 48.

42 *Id.* at 47.

43 *Id.* (emphasis in original).

should be part of the criterion, or whether other limiting factors should be defined, especially given the unique nature of cyberspace.[44]

b) Direct causation criterion

The second DPH criterion is "direct causation." This means 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."[45] How this criterion is interpreted matters deeply for tech company employees because they may engage in acts that have varying degrees of directness to any harm they may cause. For example, an employee might conduct routine and generic cyber hygiene that prevents a party to an armed conflict from conducting a cyber operation against a computer system. Or, they might share intelligence with a party to an armed conflict about specific military cyber operation being conducted by the other side. An employee might also directly remove a specific military cyber threat from a specific system or network that the employee is paid to defend. An employee might even be allowed to carry out an offensive cyber operation on a system controlled by a party to the conflict.

Whether a tech company employee carries out any of these or other activities, the ICRC Interpretive Guidance takes the position that the direct causation criterion should be understood as meaning that the harm in question must be brought about in "one causal step."[46] The guidance also explains that in the case of collective military operations, for an act to meet the direct causation criterion, it must be an "integral part" of a "coordinated military operation" that directly causes harm. The DPH experts discussed the choice of the term "integral" at length, with its proponents emphasizing that "integral part" should be interpreted narrowly to include only those acts that would "have to be an actual 'part of' and not merely a 'contribution to'" an operation.[47] The guidance explains that the criterion would be met if an act is an integral part of a concrete and coordinated tactical operation that directly causes the threshold of harm in one causal step.[48]

---

44 ICRC, FOURTH EXPERT MEETING ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER IHL (GENEVA, NOV. 27–28, 2006) SUMMARY REPORT 41–42, https://perma.cc/49R9-LJHR.

45 *See e.g.,* Denmark Manual, *supra* note 33, at 168; Norwegian Manual, *supra* note 33, ¶ 33, ¶ 3.24; U.S. Department of Defense, Law of War Manual (2015, updated July 2023) § 5.8.3, https://perma.cc/WQM7-4A5B (citing to Stephen Pomper, *Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress Through Practice*, 88 INT'L L. STUDIES 181, 189 (2012)).

46 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 53.

47 ICRC, FOURTH DPH EXPERT MEETING SUMMARY REPORT, *supra* note 44, at 47.

48 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 54–55.

Applying this criterion correctly is particularly relevant to the tech sector because of the strong public-private cybersecurity partnerships that are being built on the premise that the private sector should inform the public sector about cyber threats so that the public sector can neutralize them. Every case will need to be assessed on its facts. Only under exceptional circumstances set out above would intelligence-sharing fulfill the direct causation criteria. For example, the criterion has been interpreted to encompass gathering and passing intelligence on enemy operations provided that this gathering and transmission of information is integral to a specific cyber operation and that the operation causes the threshold of harm.[49] Conversely, the DPH experts generally agreed "that civilians merely answering questions asked by passing military personnel could not be considered as directly participating in hostilities."[50] Though the experts were not discussing cyber-related intelligence sharing, it should be deduced from this that providing generalized information to a party to an armed conflict relating to, for example, cyber hygiene or other such information that is not an integral part of a concrete and coordinated military operation that directly causes the threshold of harm, would not qualify.[51]

c) Belligerent nexus criterion

The third DPH criterion—known as the "belligerent nexus" criterion—requires that the act must be "specifically designed" to directly cause the required harm in support of a party to the armed conflict and to the detriment of another. The rule reflects IHL treaty law, which describes the term "hostilities" and individual "attacks" as activities that are directed at "injuring the enemy" and "against the adversary," respectively.[52] On that basis, the DPH guidance takes care to point out that this criterion would not be met if, for example, a large group of refugees or other fleeing civilians inadvertently blocked an access road used by the military. The guidance explains that such conduct lacks a belligerent nexus because it is not "specifically designed to support one party to the conflict by causing harm to another."[53]

The guidance also specifies that civilians do not lose their protection from attack when they are "totally unaware of the role they are playing in the conduct of hostilities" or when their acts are conducted in "self-defense or in defense of others against violence prohibited under IHL."[54] Such self-defense includes, for example, the use of necessary and proportionate force by civilians "to defend themselves against unlawful attack or looting, rape, and murder by marauding"

---

49 TALLINN MANUAL 2.0, *supra* note 6, Rule 97 ¶ 6. *See also* K. Mačák, *supra* note 37, at 974–75.

50 ICRC, SECOND DPH EXPERT MEETING SUMMARY REPORT, *supra* note 35, at 5.

51 K. Mačák, *supra* note 37, at 975.

52 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 58.

53 *Id.* at 61.

54 *Id.* at 60–61.

where its purpose "clearly is not to support a party to the conflict against another."[55] When civilians engage in such acts, similar to the blocked road example above, the acts do not meet the "specifically designed" element of the belligerent nexus threshold and, therefore, do not meet the criterion. Mačák provides compelling justifications for why it is so important that this is the end result:

> There is a wide range of situations, in which reporting the position of the enemy to the authorities is a normal (i.e., non-hostile) civilian conduct, which should not be construed as an act leading to the person's targetability. Otherwise, for instance, internally displaced persons arriving in camps would not be able to tell their stories to the government authorities if they contained information on the location of enemy forces – or a civilian air traffic controller could not report the approach of enemy military aircraft in the course of her work – without becoming targetable under IHL.[56]

Understanding the limits of the belligerent nexus criterion is important when applying it to the cyber context. The ubiquity of digital goods and services in the everyday lives of people living in situations of armed conflict and their interconnected use by civilians and militaries means that the employees of digital tech companies may inadvertently engage in acts that harm one party to an armed conflict while supporting its adversary. Such inadvertent harm may be caused when an employee defends against an unlawful attack against civilian networks in a necessary and proportionate manner; or when an employee is unable to attribute a cyber-attack but flags it nonetheless to a party to the armed conflict, not knowing that doing so would have a direct adverse effect on the opposition's military operation.[57] In both cases, applying the same logic as above, the belligerent nexus would not be met and the employee would not lose their protection from attack.

There remains, however, the challenge of how parties to armed conflict and tech company employees are to apply these considerations in practice. For

---

55 *Id.* at 61. *See also* K. Mačák, *supra* note 37, at 977. Given this formulation, it appears however that the self-defense exception to DPH could not be used to justify cyber action in defense against a lawful attack directed at a military objective that incidentally harms civilians.

Notably, some States have reinforced the ICRC's approach. The Norwegian Military Manual requires that an act must be "committed with the *intent* of causing damage to one party to a conflict for the benefit of another," and clarified that unintentional acts that harm military operations do not qualify (emphasis added). The Denmark Manual similarly indicates that intent must be accounted for. *See* Norwegian Manual, *supra* note 33 ¶¶ 3.2, 3.27; Denmark Manual, *supra* note 33, at 171; N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 61.

56 Mačák gives these examples in the context of the direct causation threshold, but they are equally relevant to the belligerent nexus threshold. In the examples he offers, they would fail the belligerent nexus threshold test when the sharing of information is not specifically designed to support one side of the conflict and to be to the detriment of the other. *See* K. Mačák, *supra* note 37, at 975.

57 Florian J. Egloff & Myriam Dunn Cavelty, *Attribution and Knowledge Creation Assemblages in Cybersecurity Politics*, 7:1 J. CYBERSECURITY 1, 5 (2021), https://perma.cc/YQZ5-NMT2 (pointing out that "attribution . . . can often be hard to substantiate with robust data").

example, when a tech company employee engages in defensive cyber activities without knowing that they will adversely affect the military cyber operations of a party to an armed conflict, how is that party to distinguish the employee's activity from activities with similar effects that were "specifically designed" to support one party of an armed conflict and be to the detriment of the other side? And if a tech company employee is told to engage only in self-defense cyber activities to protect civilians, how will the employee know whether the portion of a network used by civilians that they are responsible for defending might be a lawful target because it is being simultaneously used by a party to the armed conflict in a manner that makes it qualify as a military objective. How are parties to armed conflict and tech company employees supposed to act in such instances of uncertainty? Here are four considerations:

1) The ICRC guidance says that the determination of the belligerent nexus must be "based on information reasonably available to the person called on to make the determination, but they must always be deduced from objectively verifiable factors."[58] To avoid error or misapplication of DPH, it is therefore helpful for States to provide guidance that instructs their military cyber operators what those factors might be. 2) There is also the rule of IHL that in cases of doubt, a civilian must be presumed to be protected against direct attack.[59] 3) Additionally, for legal, operational, humanitarian, and policy considerations, parties to an armed conflict could decide to direct their operations only against objects, such as networks or computers that would fulfill the definition of "military objectives" because of their use in military operations, rather than targeting persons and risking erroneous DPH assessments that could result in civilian death and injury.[60] All of these legal obligations and policy options offer important safeguards to shield civilians from losing the protections that IHL intends to afford them. 4) And, as Section IV shows, there are additional proactive measures tech companies can take to further clarify when their employees are not engaging in DPH.

d) Temporary loss of protection

In the exceptional instances when the three narrowly construed DPH criteria are met, loss of protection lasts only "for such time" as the civilian engages in

---

58 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 63.

59 Additional (I), at art. 50(1), *supra* note 27. The Tallinn experts agreed that art. 50(1) reflects customary international law. *See* TALLINN MANUAL 2.0, *supra* note 6, at Rule 95. In support of applying the presumption of civilian status to DPH considerations, *see id.* at 75–76, with additional support from some Tallinn experts in the commentary to Rule 96.

60 However, cyber-attacks against military objectives that also provide services to civilians still pose significant potential risks, in particular when they are detrimental to critical infrastructure that supports essential civilian services such as heath, electricity, fuel, and water supplies. ICRC, THE POTENTIAL HUMAN COST OF CYBER OPERATIONS: EXPERT MEETING (NOV. 14–16, 2018) REPORT (Laurent Gisel and Lukasz Olejnik eds., ICRC, Geneva, 2019), https://perma.cc/A5B2-5W3K.

DPH.[61] This reflects IHL's fundamental principle of military necessity, which precludes engaging in hostile acts that provide no military value. How this temporal element applies to tech company employees engaging in DPH will therefore naturally reflect the duration of the employee's DPH activities. This means that loss of protection could differ between employees who engage in tasks that constitute DPH for long periods of time compared to employees who are only given specific tasks that constitutes DPH for short durations.

Similar to the three criteria, the ICRC guidance interprets this temporal element narrowly, such that protection from attack is lost only during specific acts of DPH (which includes "measures preparatory to the execution of such an act, as well as the deployment to and return from the location of its execution, where they constitute an integral part of such a specific act or operation")[62] and regained in moments in between. Some have criticized this approach for unfairly creating a "revolving door" that allows civilians who repeatedly engage in DPH to regain their protection too easily. Critics say this places civilians who engage in DPH on "a better footing than lawful combatants."[63] In response to this concern, some argue that a civilian who repeatedly participates in hostilities is targetable until such participation permanently ceases.[64]

The implication of such an expansive interpretation of the temporal element of DPH is that a tech company employee who engages in DPH, even if only infrequently during a work week from their office, might lose protection from attack not only while they engage in those specific acts of DPH, but also continuously from morning to night and at home for an extended time period.[65] This result would reduce the temporal element of DPH to being almost meaningless in most cases; and the legal distinction that IHL intentionally makes between civilians who *temporarily* lose protection and other individuals who *continuously* lose protection would all but evaporate.[66] This outcome is why the guidance explains that this revolving door is "an integral part, not a malfunction,

---

61 Protocol Additional (I) art. 51(3), *supra* note 27; ICRC CUSTOMARY LAW STUDY, *supra* note 10, at Rule 6; N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 65–68. In the cyber context, *see generally* TALLINN MANUAL 2.0, *supra* note 6, at Rule 97 ¶¶ 8–12.

62 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 65.

63 U.S. Department of Defense Law of War Manual, *supra* note 45 § 5.8.4.2.

64 *Id.* § 5.8.4.1.

65 This analysis presumes that the employee is a civilian and has not lost that status by virtue of serving a "continuous combat function" in a non-international armed conflict or from qualifying as a combatant in an international armed conflict. For more details on this issue, *see* N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 27–40, in particular the discussion around contractors and civilian employees working for parties to an armed conflict.

66 *Id.* at 44–45; Nils Melzer, *Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 N.Y.U. INT'L L. POL. 831, 890 (2010).

of IHL. It prevents attacks on civilians who do not, at the time, represent a military threat."[67] In summation, while the application of the temporal element of DPH to tech company employees will hinge on the operational realities of their tasks, it is equally clear that an expansive interpretation of "for such time" would expose civilian tech workers to attack during the times when IHL intended them to be protected civilians.

The use of artificial intelligence and autonomy in cyber capabilities may raise additional temporal factors to consider. For example, an employee might activate automated tasks or autonomous systems that patch vulnerabilities or find vulnerabilities to exploit. These tasks may then persist without requiring the employee to take any further active role. If activating such tasks qualify as DPH, does the employee's loss of protection conclude at the conclusion of the task, or at the end of the employee's active role in the task? It has been persuasively argued that the end of DPH is dependent on the end of the worker's active role and not on the duration of the task. The reasoning for this is that after the worker ends their active role there is no longer a justification for targeting them because they are no longer directly participating in the activity.[68]

e) Concluding considerations

The cyber context illustrates that there remains room for States to provide further clarity on the contours of DPH.[69] But it remains true that parties to armed conflict must comply with their obligations under IHL, including the principle of distinction when it comes to tech company employees. This means adhering to the purposefully narrowly formulated DPH criteria so not to mislabel protected civilians as civilians who may be attacked. It means complying with IHL's obligation to do everything feasible to verify whether a civilian has lost protection from attack.[70] When situations of doubt arise as to whether a civilian is engaging in DPH, it also means presuming they are not doing so.[71] As will be discussed in Section III, adherence to these principles and rules of IHL also helps reduce "digital crossfire" that puts other civilians at risk of being incidentally harmed.

---

67 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 70. In further defense of the ICRC interpretation, *see id.*, at 888–92.

68 ICRC, EXPERT MEETING ON AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS, *supra* note 40, at 32. *See also* ICRC, *Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach*, 102 INT'L REV. RED CROSS 463, 467 (2020). *See also*, K. Mačák, *supra* note 37, at 980–81; TALLINN MANUAL 2.0, *supra* note 6, at Rule 97 ¶ 9.

69 TALLINN MANUAL 2.0, *supra* note 6, at Rule 97 ¶ 6. Brazil, for example, has said the issue of DPH in the cyber context deserves "further reflection." *See* G.A. Res. 73/266, at 23 (July 13, 2021), https://perma.cc/Y5WH-KQSS.

70 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 16.

71 In support of applying the presumption of civilian status to DPH considerations, *see* N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 6, at 75–76; TALLINN MANUAL 2.0, *supra* note 6, at Rule 96.

Finally, as set out in Section IV, there are also measures tech companies can take—and may be obligated to take—to advance IHL's aim to protect civilians against dangers arising from military operations.

2. Company properties, civilian objects, and military objectives.

This part focuses on how the principles and rules of IHL protect the properties of private digital tech companies. The principles and rules most relevant to this discussion are those prohibiting attacks against civilian objects and regulating those against military objectives.[72] Recall from above that the properties of a tech company might include offices, factories, warehouses, computers, printers, desks, routers, modems, fiber optic cables, and other hardware, software, network infrastructure, and data. Given its vastness, companies have considerable interest in understanding how IHL applies to their properties when operating in the context of an armed conflict. One expert has gone so far as to foreshadow that cyber operations "misattributed to innocent civilian assets and systems makes distinction of means far more important than distinction of personnel launching attacks."[73]

Under the principle of distinction, IHL prohibits attacks directed against civilian objects but does not prohibit attacks against military objectives.[74] In so far as objects are concerned, military objectives are "limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[75] Determining whether a piece of tech company property qualifies as a military objective requires that it be assessed against this definition. When it comes to

---

72 Assessing whether tech company property qualifies as a "civilian object" or "military objective" is not, however, the only way to assess how IHL might protect such property. For example, distinct from the rules protecting civilian objects against attack, IHL also prohibits the destruction or seizure of the property of an adversary, unless required by imperative military necessity. The property protected is both private and public. The specific rules can vary depending on circumstances, but suffice it to say that in situations of armed conflict a tech company's property, including its data, could be at risk of seizure or destruction by a party to the armed conflict. The U.S. Department of Defense Law of War Manual acknowledges this and explains that it is possible to apply the rules of seizure and destruction to the cyber context. The Manual adds, however, that "challenging issues may arise" in applying those rules in the cyber context. Whatever those challenges may be, the overarching implication is that if a tech company's data holds no military value, then it cannot be seized or destroyed. *See* ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 50; Sigrid Redse Johansen, *Destruction and Seizure of Property When Military Necessity Requires, in* THE MILITARY COMMANDER'S NECESSITY: THE LAW OF ARMED CONFLICT AND ITS LIMITS 341–362 (Cambridge Univ. Press, 2019); DoD Law of War Manual, *supra* note 45 §§ 5.17.5, 16.2.1.

73 Sean Watts, *Combatant Status and Computer Network Attack*, 50:2 VA. J. INT'L L. 391, 442 (2010), https://perma.cc/MZQ3-E8LQ.

74 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 7.

75 *Id.* at Rule 8.

"objects," if a piece of property does not fall within the scope of the definition of a "military objective" then IHL regards it as a "civilian object" and, as such, prohibits attacks from being directed at it.[76] If it does fall within the definition, it may be attacked, provided other principles and rules of IHL are complied with.[77]

Loss of protection has consequences that extend beyond the tech companies. This is also important for the companies to keep in mind. Military objectives, when targeted, expose proximate civilians and civilian objects to risks of incidental harm that IHL may not prohibit. For example, if a piece of tech company property qualifies as a "military objective" it may still be targeted in some circumstances even if civilians rely on it to receive essential services.[78]

All of these consequences demand a clear understanding of how to assess whether, and if so which, piece or pieces of tech company property qualify as a civilian object or military objective.

A "military objective" is not meant to refer to the general or abstract objective of a military action (e.g., its aim, purpose, or goal), but—as far as company properties are concerned—it relates to specifically identifiable pieces of a company property that may be targetable (e.g., specific buildings and computer hardware, and arguably also software).[79] It would also be inaccurate to assess a company, as a whole, as a military objective. A company is an abstract legal entity and not an "object" as understood by IHL. And even if some company buildings or other assets qualify as military objectives, this will usually not be the case for all of a company's properties. It is very unlikely that a company's total property will qualify as a military objective. This may be the case only if every one of its pieces of property fulfill the definition of a military objective.[80] The *Tallinn Manual 2.0* put a particular emphasis on this point, pointing out that "an entire computer network does not necessarily qualify as a military objective based on the mere fact that an individual router so qualifies;" and that in the context of social media platforms used for military purposes, "their military use does not mean that Facebook or Twitter as such may be targeted; only those components thereof used

---

76 *Id.* at Rule 9.

77 *Id.* at Rule 7.

78 For further discussion of this issue, *see* Section III below.

79 *See* ICRC, COMMENTARY ON THE ADDITIONAL PROTOCOLS ¶¶ 2007–10 (Yves Sandoz, Christophe Swinarski and Bruno Zimmerman eds., ICRC 1987); TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶ 4. On whether software qualifies as an object that may qualify as a military objective, *see* the discussion of "data" in L. Gisel et al., *supra* note 35, at 317–20.

80 *See generally* ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 7. Speaking further to the obligation to direct attacks against specific objectives rather than entities as a whole, *see* TALLINN MANUAL 2.0, *supra* note 6, at Rule 101 ¶ 6 ("virtually any attack against the Internet would have to be limited to a discrete segment thereof"); E. Mavropoulou, *supra* note 35, at 46 ("Simply put, the systemic interconnectivity renders the whole cyber domain a potential dual-use target, at least in theory. However, the view that the whole cyber domain can be a military objective by use is somewhat farfetched and one-sided.").

for military purposes may be attacked,"[81] provided they meet the definition of military objective.

When judged in light of the definition of a military objective, objects that tech companies own that are exclusively used for civilian purposes do not fall within the scope of the definition. IHL would prohibit, for example, an attack against objects that exclusively maintain the operating system of a water treatment facility that constitutes a civilian object.[82] International humanitarian law would also prohibit attacking objects that exclusively provide services to specifically protected entities under IHL, such as hospitals.[83] It is also well-accepted under IHL that objects do not constitute military objectives when they merely generate support for the war effort or boost civilian morale and nothing more. Such objects owned and operated by social media companies would therefore benefit from that same protection.[84]

A more complex example is where a piece of tech company property (e.g., computer consoles) is used to defend against an unlawful military operation against the civilian population. In the author's view, if such a piece of property were used solely to protect the civilian population from such an attack and caused no harm other than thwarting the operation, it would be absurd for that property to qualify as a military objective. Such a result would imply that the use of civilian property solely to defend a civilian population against unlawful attacks would constitute an "effective contribution to military action" and that destroying it would provide a military advantage. This result is plainly antithetical to the principle of distinction, which prohibits attacking civilians and civilian objects precisely because they do not contribute to military action and their destruction offers no military advantage. Similarly, it is not enough to claim that any piece of tech company property used by the military is a military objective. Networks used by the military for personal or other non-military use would not qualify as military objectives if they do not make an effective contribution to military action or when attacking them provides no military advantage.[85]

---

81 TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶ 10; Rule 101 ¶ 5.

82 ICRC, Cyber Operations in Armed Conflict: The Principle of Distinction (Mar. 2023), https://perma.cc/W45Z-XQKG.

83 L. Gisel et al., *supra* note 35, at 327–28.

84 *See* International Criminal Tribunal of the former Yugoslavia prosecutor's office, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia ¶ 47 (June 13, 2000), https://perma.cc/2RTL-XFEY ("Whether the media constitutes a legitimate target group is a debatable issue. If the media is used to incite crimes, as in Rwanda, then it is a legitimate target. If it is merely disseminating propaganda to generate support for the war effort, it is not a legitimate target."); TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶ 15.

85 In support of this view, but also for alternative views, *see* TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶¶ 27–28.

On the other hand, examples of pieces of tech company property that may qualify as military objectives include specific pieces of cyber infrastructure that provide a party to an armed conflict command and control capabilities for military operations,[86] surveillance,[87] or intelligence sharing platforms.[88] For an object to qualify as a military objective, it does not matter who the object belongs to; it therefore does not matter if the piece of property in question is owned by the State or a private company.[89] The *Tallinn Manual* experts similarly agreed that a factory that produces hardware or software under contract to the enemy's armed forces would also constitute a military objective; a position this author agrees with provided the factory fulfills the full definition of military objective and the hardware or software is not, for example, used for detainee management or military medical services.[90]

It also does not matter whether the object is used offensively or defensively for it to qualify as a military objective. Tech company computers used to repel military cyber intruders that have entered an adversary's network and tech company computers used to plant malware into a military's operating system could both qualify as a military objective if they met the definition. A piece of property may also constitute a military objective due to its relationship with another military objective. A scenario can be imagined where a cyber-attack is directed at a privately owned civilian aviation air traffic control tower that the enemy military temporarily uses to enable offensive air operations. In this example, the air traffic control tower might qualify as a military objective because of its "use" in relation to other military objectives, namely the enemy fighter jets.

The protections that IHL affords tech company property may also have to be assessed in situations where civilians and the military are mutually reliant on the same piece of property. These can be difficult cases to assess, but they can be a common feature in today's armed conflicts due to the intertwined and unsegregated nature of military and civilian networks.[91] Imagine the case of a company that runs a single server that detects and deters malware on civilian and military operating systems. This carries certain risks for the company since under IHL such a server may constitute a military objective despite it also providing

---

86 *Id.* at Rule 100 ¶ 8; E. Mavropoulou, *supra* note 35, at 42.

87 TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶¶ 27–28.

88 *Id.*

89 *Id.*

90 *Id.* at Rule 100 ¶ 11 (caveating that "a factory producing items that the military only occasionally acquires is not a military objective," and that a difficult case "involves a factory that produces items that are not specifically intended for the military, but which are frequently put to military use.").

91 *See* E. Mavropoulou, *supra* note 35, at 42 ("[T]he inherent structure of cyber space provides no foolproof segregation of private, military and civilian networks."); Kubo Mačák & Laurent Gisel, *Grammar: Rules in a Cyber Conflict, in* A LANGUAGE OF POWER? CYBER DEFENCE IN THE EUROPEAN UNION 60, 61–62 (Patryk Pawlak & François Delerue eds., Chaillot Paper, EUISS, Paris, 2022).

services to civilians.[92] "Dual-use" services could similarly arise when a tech company enables the functioning of infrastructure that provides power to the civilian population and a military base. If a party determines that the power provides an effective contribution to its enemy's military action and that a power cut would provide it with a definite military advantage, and provided other principles and rules of IHL are complied with, it may decide to attack the electric grid or the utility company with air power to no consequence of the tech company. But it also may decide to direct an attack against relevant pieces of the tech company if this accomplishes the same effect as the power cut.[93]

The shared use of cyberspace by civilians and militaries also highlights the importance of ensuring that an assessment of whether an object is a military objective must be based on whether the object's destruction, capture, or neutralization provides a direct military advantage determined by the *circumstances ruling at the time*. To illustrate this point, the *Tallinn Manual 2.0* uses the example of a civilian air traffic control system that is temporarily used for military purposes before returning to be used exclusively for civilians. While the system may have qualified as a military objective whilst used by the military, *Tallinn Manual 2.0* explains that it ceased being so once it returned to providing exclusively civilian functions.[94]

As seen, "military objective" is a legal term of art with a dynamic definition. The interconnectivity between cyber space, tech company goods and services, and those living and operating in situations of armed conflict—whether as civilians or opposing militaries—may produce complex environments that make it particularly important to determine whether pieces of tech company property are protected from attack or whether some of them may qualify as a military objective. Though not covered in this paper, this operational landscape is made more complex by legal debates over what constitutes an "attack" under IHL and what protections IHL affords data.[95] Because of these complexities, it will be important that parties to armed conflict comply with their obligations under the principle of distinction as well as their related obligation to do everything feasible to verify

---

92 *See* TALLINN MANUAL 2.0, *supra* note 6, at Rule 101. *See also* E. Mavropoulou, *supra* note 35, at 45–48.

93 The attack also would have to comply with IHL's other principles and rules regulating conduct of hostilities, in particular the prohibition against indiscriminate and disproportionate attacks, and the obligations to take precautionary measures. With regard to precautionary measures, in this scenario it may be particularly important to recall the rule that "When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected must be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects." *See* ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rules 11–21. For further discussion of these principles and rules, *see* Section III below.

94 TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶¶ 12, 24.

95 *See* L. Gisel et al., *supra* note 35, at 312–20.

whether an object qualifies as a military objective.[96] Given the potential for military objectives to revert back to civilian objects,[97] these assessments and verifications cannot be one-offs, but must be valid based on the circumstances ruling at the time. And when situations of doubt arise as to whether an object normally dedicated to civilian purposes is being used to make an effective contribution to military action, it must be presumed as not doing so.[98] Additionally, as discussed in Section III below, parties to armed conflict must comply with IHL's prohibition on indiscriminate and disproportionate attacks and its obligations to take all feasible precautions to avoid or at least minimize incidental civilian harm, which includes damage to civilian objects. Finally, and as discussed in Section IV, tech companies can and should take—and may be obligated to take—steps that reduce risks to themselves and surrounding civilians.

3. Relationship between company employees and properties.

To further understand the implications that arise under the principle of distinction when tech companies operate in situations of armed conflict, it is helpful to examine how IHL treats employees who use pieces of company property that qualify as military objectives. It is similarly helpful to examine how the law treats company property that employees use when they are engaged in DPH. There is nothing particularly unique about these symbiotic relationships between people and objects when applied to tech companies in wartime. But examining their legal relationship demonstrates that we must not conflate the two distinct tests for determining when tech company employees and pieces of company property lose their protection against attack.

To demonstrate this point, take the example of a tech company building where employees are contracted to develop military cyber weapons to be used by a party to an armed conflict. It is widely agreed that a factory that produces munitions for a party to the conflict may be liable to attack because it qualifies as a military objective as the munitions factory makes an effective contribution to military action and its destruction would offer a definite military advantage.[99] The same then could be said of the building where the cyber weapons are being developed. At the same time, however, it is generally agreed upon and State practice demonstrates that the civilian workers making the munitions are not

---

96 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 16.

97 TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶¶ 12, 24.

98 Additional Protocol I art. 52(3), *supra* note 27. The majority, but not all, of the Tallinn experts agreed that art. 52(3) reflects customary international law. For a further discussion of how this rule applies to objects and associated cyber infrastructure, *see* TALLINN MANUAL 2.0, *id.* at Rule 102.

99 *But see* TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶ 11 (caveating that "a factory producing items that the military only occasionally acquires is not a military objective").

engaging in DPH.[100] The same reasoning applies to the tech company employees producing the cyber weapons. As long as the production of the weapons is not an integral part of a specific concrete and coordinated military operation that directly causes the harm, they would not meet the DPH direct causality criterion.[101]

It is also possible to test the proposition that an object does not necessarily qualify as a military objective when a civilian is using it to engage in DPH. Imagine the case of a tech company employee who is engaging in DPH when using a dedicated company server to design bespoke malware to disrupt a command-and-control system being used by a party to the armed conflict. In these circumstances, it would be reasonable to conclude the server is making "an effective contribution to military action."[102] The server would, therefore, meet the first element of the definition of a military objective. But that is only one part of the analysis. The partial or total destruction, capture or neutralization of the server must *also* be expected to offer a "definite military advantage" in the circumstances ruling at the time.[103] This is where cyberspace's unique quality of resiliency through redundancy amplifies the importance of the second part of the definition. Let us say the employee's company has server redundancy and the employee is able to continue designing the malware uninterrupted when the primary server is attacked. The question then arises whether an attack against the server could be expected to yield a definite military advantage when the employee continues to operate unimpeded? If such advantage cannot be expected, then the server would not qualify as a military objective.[104]

---

100 N. MELZER, ICRC, INTERPRETIVE GUIDANCE, *supra* note 24, at 53. For State views, *see*, *e.g.,* UK Ministry of Defense, *The Joint Service Manual of the Law of Armed Conflict*, 2004 ¶ 2.5.2 ("Thus working in a munitions factory or otherwise supplying or supporting the war effort does not justify the targeting of civilians so doing."); Denmark Manual, *supra* note 33, at 170 (saying there is no direct causal link in cases of "[p]articipation in the production and transport of weapons and other military equipment unless such support is provided for specific military operations").

101 If the building were attacked, civilian workers may, however, suffer harm incidentally. Whether IHL prohibits such harm will depend on whether the attack on the building complied with the prohibition on indiscriminate attacks and the principles of precaution and proportionality. For further discussion of these issues, *see* Section III below.

102 Of the four separate criterion that can make an object a military objective (e.g., location, nature, purpose, or use), the network could reasonably fall under either/or the "use" or "purpose" criterion. Under IHL, "use" refers to what the object is being used for at the moment of attack, whereas "purpose" refers to the object's intended future use. TALLINN MANUAL 2.0, *supra* note 6, at Rule 100 ¶¶ 10, 13–14.

103 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 8.

104 *See* ICRC, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS, 42 (Geneva, 2015) (". . . because cyberspace is designed with a high level of redundancy, one of its characteristics is the ability to immediately reroute data traffic. This inbuilt resilience needs to be taken into account when assessing whether the target's destruction or neutralization would actually offer a definite military advantage in the circumstances ruling at the

III. EXPOSING CIVILIANS TO "DIGITAL CROSSFIRE"

When tech companies operate in situations of armed conflict, it is not only their employees and property that may face the dangers of attack. This paper touched on this issue above in its discussion around "dual-use" military objectives. It is worth expanding on. The intermingled and interconnected relationship that tech companies have with civilian populations may also expose the latter to the harms of digital crossfire, in particular harms that IHL aims to avoid or minimize but may not prohibit. Such harm might be caused by a kinetic airstrike that incidentally kills or injures civilians or damages or destroys civilian objects located in close physical proximity to a tech company building that qualifies as a military objective. Similarly, incidental civilian harm might result from a belligerent cyber-attack aimed at damaging tech company infrastructure that both supports the belligerent's adversary and is necessary for providing essential services to the civilian population through digital means.[105]

This conclusion may seem counterintuitive to IHL's aim to ensure respect for and protection of the civilian population and civilian objects in situations of armed conflict.[106] But it is equally true that IHL tolerates a certain degree of incidental civilian harm, in particular when attacks are directed at military objectives and persons who are not protected against attack, including civilians engaging in DPH. Provided that parties fulfil all their IHL obligations, in particular to take all feasible precautions to avoid, or at least minimize, incidental death and injury of civilians and damage to civilian objects (hereafter referred collectively to as "incidental civilian harm"),[107] an attack may not be prohibited if the incidental civilian harm is not expected to be "excessive" in relation to the attack's anticipated concrete and direct military advantage.[108] This is why a company's involvement in an armed conflict runs a risk of exposing civilians and civilian

---

time, as required by the second prong of the definition of a military objective."). *See also* E. Mavropoulou, *supra* note 35, at 43–44 (similarly explaining, "Cyberspace is relatively resilient compared to other targets. In the case of an attack against a cyber infrastructure such as communication networks, 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 the intended destination. 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. Only if all possible or at least the major communication paths are destroyed, might an advantage effectively be gained and this is without prejudice to future real-life scenarios.").

105 *See* ICRC, Working Paper on Constraints under International Law on Military Operations in, or in Relation to, Outer Space during Armed Conflicts 2 (May 3, 2022). *See also*, Tallinn Manual 2.0, *supra* note 6, at Rule 113 ¶ 4.

106 Additional Protocol I art. 48, *supra* note 27.

107 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rules 15–21.

108 *Id.* at Rule 14. *See also* TALLINN MANUAL 2.0, *supra* note 6, at Rule 113 ¶ 2 ("[T]he fact that civilians or civilian objects suffer harm during a cyber attack on a lawful military objective does not necessarily render said attack unlawful *per se*.").

objects to dangers they otherwise may not face. It is also another reason why interpretations of DPH and "military objective" matter so much. Broad interpretations of these terms would lead to more people and objects being regarded as lawful targets, which increases the potential for civilians to get caught in digital crossfires. Conversely, narrow interpretations reduce the number of lawful targets, which reduces that risk.

The tolerance that IHL has for incidental civilian harm must not, however, be overstated. States wrote IHL's rules against indiscriminate attacks and its principles and rules of precaution and proportionality in purposefully broad and protective terms. States have widely agreed that these same principles and rules apply to cyber-attacks in situations of armed conflict.[109] By way of example, an indiscriminate cyber-attack is one that is not directed at a specific military objective, employs a method or means of combat which cannot be directed at a specific military objective, or employs a method or means of combat the effects of which cannot be limited as required by international humanitarian law.[110] Setting loose a "worm" (a self-replicating or self-propagating computer program) that damages anything it encounters with the hope that it eventually damages an adversary's computer network would, therefore, be prohibited as an indiscriminate attack under IHL.[111] International humanitarian law would also arguably regard as indiscriminate (and in any case violating the obligations of precautions, discussed below) an attack damaging a cloud server that co-locates its services to civilians and a military adversary, provided that it would be feasible to have instead attacked clearly separated and distinct parts of the server that constituted military objectives.[112]

The principles and rules of precaution and proportionality provide additional guardrails in IHL that further aim to avoid, or at least minimize, incidental civilian harm. The ICRC has taken the view that when applying the obligations of precaution and proportionality, all foreseeable incidental civilian harm—both

---

109 *See e.g.*, G.A. Res. 73/266, *supra* note 69, at 22–23 (Brazil), 36–38 (Germany), 60 (Netherlands), 94 (Switzerland). *See also* Government of Canada, International Law Applicable in Cyberspace ¶ 49, https://perma.cc/6JVB-R3XX.

110 ICRC, CUSTOMARY LAW STUDY, *supra* note 10, at Rule 12.

111 Germany takes the position, "Thus, computer viruses designed to spread their harmful effects uncontrollably cannot distinguish properly between military and civilian computer systems as is required under IHL and their use is therefore prohibited as an indiscriminate attack." German position, *supra* note 33, at 9. *See also* Jonathan Horowitz, *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC Issue*, ASIL INSIGHTS, May 19, 2020, https://perma.cc/QGA5-Y3FM.

112 *See* TALLINN MANUAL 2.0, *supra* note 6, at Rule 112 ¶ 2.

direct and indirect—must be considered.[113] This is a position States generally agree with.[114] Direct civilian harm relates to consequences that are directly and immediately caused by a cyber-attack. All other civilian harm is considered indirect harm; sometimes referred to as the "reverberating" effects of an attack.[115] For example, if it is reasonably expected that a cyber-attack against a commercial satellite used by the military will also result in damage to merchant vessels and civil aircraft that rely on it, all feasible precautions must be taken to avoid, or at least minimize that damage. If those harms cannot be avoided, that damage must be part of the proportionality assessment to ensure the attack is not disproportionate.[116] And if the attack is expected to be disproportionate, it cannot go forward.[117]

The standard for assessing incidental civilian harm is based on an *ex-ante* standard of "foreseeability."[118] Importantly, the principles and rules of precaution and proportionality do not place geographic or temporal limits on the incidental civilian harm that parties to an armed conflict must take into account.[119] Even transborder harm that is expected to occur in non-belligerent States needs to be accounted for.[120] In comparison, the "military advantage" that is weighed against incidental civilian harm under the proportionality principle is that which is "concrete and direct," meaning it has a narrower scope. The drafting history of Additional Protocol I shows that these terms were used to confine military advantage to that harm which is "substantial and relatively close, and that advantages which are hardly perceptible and those which would only appear in the

---

113 *See* ICRC, 2015 Challenges Report, *supra* note 104, at 41–44, 50, 52; ICRC, THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW: REPORT OF INTERNATIONAL EXPERT MEETING (JUNE 22-23, 2016) 43–45 (Laurent Gisel ed., ICRC, 2018); Emanuela-Chiara Gillard, *Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment* ¶¶ 48–58, 61–69 (Chatham House, 2018); Tallinn Manual 2.0, *id.* at Rule 113 ¶¶ 6–7.

114 While a number of military manuals and other relevant official State documents also require the consideration of indirect harmful effects, others have taken a narrower view that the harms are generally understood to refer only to harms that are "immediate or direct." *See e.g.*, DoD Law of War Manual, *supra* note 45 § 5.12.1.3.

115 ICRC, EXPERT MEETING ON THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW, *supra* note 113, at 43–45; and E. Gillard, *supra* note 113 ¶ 61–69.

116 TALLINN MANUAL 2.0, *supra* note 6, at Rule 113 ¶ 4.

117 *Id.*; ICRC CUSTOMARY LAW STUDY, *supra* note 10, at Rules 14 and 19.

118 ICRC, EXPERT MEETING ON THE PRINCIPLE OF PROPORTIONALITY IN THE RULES GOVERNING THE CONDUCT OF HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW, *supra* note 113, at 43–45; E. Gillard, *supra* note 113 ¶¶ 48–58.

119 E. Gillard, *supra* note 113 ¶ 63.

120 *See* Jonathan Horowitz and Florentina Pircher, *Scenario 28: Extraterritorial incidental civilian cyber harm*, CYBER LAW TOOLKIT, https://perma.cc/EM2H-AEB7.

long term should be disregarded."[121] The expected military advantage assessed therefore cannot be merely speculative. The tolerance IHL has for civilian harm also hinges on what qualifies as "damage" to civilian objects and what protections IHL affords civilian "data." Without addressing those two definitional issues further, suffice it to say that narrow protective interpretations will allow for greater civilian harm, whereas broader protective interpretations tolerate less.[122]

IV. RECOMMENDATIONS TO COMPANIES: TRAIN, ASSESS, MITIGATE, INFORM

Having set out some of the legal implications that arise when tech companies provide digital goods and services in situations of armed conflict, this paper concludes by offering recommendations for those tech companies to consider. The assumption behind these recommendations is that alongside parties to armed conflict, these companies can and should play a role in protecting civilians and civilian objects against the dangers of cyber and other military operations.

While only a short initial exploration, these recommendations build off of the United Nations Guiding Principles on Business and Human Rights and the emphasis that the UN mandated Working Group on Business and Human Rights places on the need for companies to adopt conflict sensitive approaches and heightened due diligence to identify, prevent, mitigate, and account for how they address their adverse impacts.[123] Some of these recommendations may in fact reflect legal obligations or liabilities that companies already have under national laws. At the same time, if a tech company does not follow this paper's recommendations, this would not absolve the warring parties from complying with their obligations under IHL, in particular, the prohibition against directing attacks against protected civilians and objects, the prohibition against indiscriminate and disproportionate attacks, and the obligation to take all feasible precautions to avoid or minimize incidental civilian harm, as well as the obligation to do everything feasible to protect civilians and civilian objects under their control from the effects of an adversary's attack.[124]

---

121 *See* ICRC, COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 79 ¶ 2209. For a discussion of different State interpretations of this requirement, *see* ICRC, CUSTOMARY IHL STUDY, *supra* note 10, at Rule 14; WILLIAM H. BOOTHBY, THE LAW OF TARGETING 94–95 (Oxford Univ. Press, 2012).

122 *See* L. Gisel et al., *supra* note 35, at 312–20.

123 *Supra* notes 4 and 5.

124 For a discussion on States' obligations to take precautions against the effects of cyber-attacks, *see* ICRC, EXPERT MEETING ON AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS, *supra* note 40, at 7, 27–28, 54; Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions*, 89 INT'L L. STUD. 198, 211–16 (2013).

A. IHL Knowledge and Understanding

Company decision-makers should familiarize themselves with necessary understandings of IHL as they relate, in particular, to the notion of "direct participation in hostilities," "attacks," "military objectives," and "civilian objects."[125] This could be accomplished through IHL training programs that help them understand the implications that the basic rules and principles of IHL have for their company's activities in situations of armed conflict. States could also promote this educational measure as part of their obligation to encourage the teaching of IHL and to ensure respect for IHL.[126] Having this understanding and knowledge of IHL will be key for company policy makers and lawyers to conduct IHL assessments and make proper use of their findings, which is the next recommendation.

B. IHL Protection Assessments

For tech companies to understand some of the most consequential IHL implications of their activities, companies should audit or otherwise assess whether any of their employees are engaging in DPH and whether any of their properties qualify as military objectives. Doing so may be particularly relevant for companies that support critical infrastructure, own communications and cloud computing services, provide cyber defense services, and design and produce other cyber tools and capabilities that may be used militarily in situations of armed conflict.

C. Risk Mitigation Measures

If a company wants to retain IHL's legal protections against attack for its employees and properties, it should ensure its employees do not engage in DPH and that its properties do not qualify as military objectives.

While it is the obligation of belligerents to do everything feasible to verify that its targets are military objectives, companies that engage solely in civilian activities could also consider making information about those activities available to warring parties. This might help prevent targeting errors and mitigate civilian

---

125 Q&A: International Humanitarian Law and Business, *Ten questions to Philip Spoerri, ICRC Director for International Law and Cooperation*, 94 INT'L REV. RED CROSS 1125, 1127 (Autumn 2012), https://perma.cc/LD8J-QSU3 (". . . it remains possible that, in the context of an armed conflict, business activities will become linked with the hostilities – for instance, if an enterprise provides support to a party to the conflict or if some staff of the enterprise are members of an armed group of a party to the conflict. It is thus important for a company manager to be aware of IHL rules and of their scope of application to avoid possible violations and/or complicity in violations by others.").

126 ICRC, CUSTOMARY INTERNATIONAL LAW STUDY, *supra* note 10, at Rule 143; ICRC, COMMENTARY ON GC III, *supra* note 20, ¶ 184.

harm by countering misunderstandings over whether a company's employees or any of its properties are liable to attack by belligerents.

Companies engaged solely in civilian activities could also make available to warring parties information about incidental civilian harm that may be directly or indirectly caused by a belligerent attack. Parties to an armed conflict would be legally obligated to take this information into account to ensure their attacks are not disproportionate. This information also helps warring parties assess what precautionary measures to take to avoid or minimize civilian harm.

While there are urgent humanitarian and practical reasons why civilians, including private company employees, should not engage in DPH,[127] if a company nonetheless employs workers to DPH, those employees must comply with relevant rules of IHL.[128] Notably, for example, civilians are liable under international criminal law if their acts constitute violations of IHL that amount to war crimes.[129]

To minimize incidental civilian harm, these companies may also need to act consistently with IHL's rules on taking precautions against the effects of attack.[130] The rule requires parties to take all feasible measures, even in peacetime, to avoid placing civilians who are under their control in harm's way. It is a rule based on the simple notion that civilians are safest when not exposed to the dangers of conflict. One way a tech company could avoid putting civilians in harm's way could be to segment the goods and services it provides to militaries from those used by civilians to reduce the risk of incidental civilian harm.[131]

D. Inform Workers and Customers

This paper has explained that the decisions a tech company makes about the goods and services it provides in situations of armed conflict have the potential to place its employees, its civilian customers, and other proximate civilians in harm's way. Companies should therefore, at a minimum, be transparent and alert employees of potential worker safety risks they might face when performing tasks that may qualify as DPH or working in facilities that may qualify as military objectives. Companies should also, as much as possible, be transparent about the

---

127 For more on this topic, *see* K. Mačák, *supra* note 37, at 965–91.

128 *See* ICRC, COMMENTARY ON GC III, *supra* note 20 ¶¶ 183–85. For obligations on prosecuting war crimes in the context of non-international armed conflict, *see* ¶ 918 and ICRC, CUSTOMARY IHL STUDY, *supra* note 10, at Rule 158.

129 ICRC, CUSTOMARY IHL STUDY, *supra* note 20, at Rule 156.

130 Additional Protocol I art. 58, *supra* note 27.

131 *See* ICRC, 2015 Challenges Report, *supra* note 104, at 43; ICRC, EXPERT MEETING ON AVOIDING CIVILIAN HARM FROM MILITARY CYBER OPERATIONS, *supra* note 40, at 54; ICRC, Preliminary recommendations on possible norms, rules and principles of responsible behaviours relating to threats by States to space system, 3 (Jan. 27, 2023).

incidental harms their civilian customers and other proximate civilians might face when those companies' digital goods or services are being used in armed conflict.

V. CONCLUSION

It is the parties to an armed conflict that are primarily responsible for complying with IHL, which includes protecting civilians from harm, whether the harm arrives though digital or more conventional means. At the same time, the ubiquity of the digital environment is increasingly bringing tech companies into contact with the realities of war. As companies find themselves involved in armed conflicts, and the lives of people living through those conflicts, they will have to decide how to navigate this space. To do this, IHL provides rules of the road that companies will need to be familiar with. IHL offers protections to a company's civilian employees and properties from attack. But it is also the choices of a company that can influence when those protections may cease and when civilians may be exposed to the crossfire of armed conflict.

This paper focuses on when and how those protections apply and when and how those protections may be lost, in particular in the narrow and exceptional circumstances when employees are engaging in DPH and when pieces of company property qualify as military objectives. The paper also reminds us how that loss of protection may put surrounding civilians and civilian objects at risk of incidental harm that IHL aims to avoid or minimize but may not prohibit. This paper further demonstrates that broad interpretations of DPH and "military objective" hold the potential to significantly expand the number of targets on the battlefield, both in the physical world and in cyberspace, and correspondingly expand the risk of collateral damage further, beyond the object and purpose of IHL.

Finally, this paper recommends to tech companies operating in conflict environments that they should familiarize themselves with IHL; assess the IHL implications of their activities; develop policies aimed at mitigating harm to workers, properties, and surrounding civilians; and inform workers, civilian customers, and other proximate civilians about dangers they might face. These recommendations, which are additional to the obligations that IHL places on parties to armed conflicts, offers a path that can help digital tech companies support the fundamental humanitarian aim of IHL to protect civilians and civilian objects from the dangers of armed conflict.