Humanity In War

WORKSTREAM 6	工作领域 6
# UPHOLDING INTERNATIONAL HUMANITARIAN LAW IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES DURING ARMED CONFLICTS	# 武装冲突期间使用信息和通信技术时维护国际人道法
BACKGROUND PAPER*	背景文件*

* This background paper was originally prepared for the first state consultation, with only minor corrections and updates made as of September 2025.

* 本背景文件原为第一轮国家咨商编写，仅于 2025 年 9 月微作调整并更新。

INTRODUCTION

The increasing use of information and communication technologies (ICTs) during armed conflicts raises significant humanitarian and legal questions. While it is widely accepted that international humanitarian law (IHL) imposes limits on the use of ICTs in armed conflict, the specificities of the ICT environment give rise to complex questions regarding its implementation. States have recognized the need for continued discussions on these questions. The ICT workstream is part of an ongoing effort to foster shared understandings.

前言

信息和通信技术（以下简称“信通技术”）在武装冲突期间的使用日益增多，这带来了重大的人道和法律问题。虽然国际人道法对武装冲突中信通技术的使用施加限制已获得普遍接受，但是信通技术环境的特性仍在实施层面引发了复杂问题。各国已经认识到，有必要就这些问题持续进行讨论。信通技术工作领域正是为促进各方达成共识而持续努力的领域之一。

I. THE USE OF ICTS IN ARMED CONFLICTS AND IHL: GLOBAL DISCUSSIONS AND EMERGING SHARED UNDERSTANDINGS	一、武装冲突中信通技术的使用：全球性讨论和正在形成的共识
The application of international law, including IHL, to ICT activities has been the subject of multilateral discussions for nearly two decades. In 2021, the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (GGE) noted by consensus that "international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognized the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict." [1] The Open-ended Working Group (OEWG) on Security of and in the Use of Information and Communications Technologies 2021–2025 echoed this conclusion in its reports.[2]	近二十年来，将国际人道法等国际法适用于信通技术活动一直是多边层面讨论的主题。2021 年，"从国际安全角度促进网络空间负责任国家行为政府专家组"（简称"政府专家组"）达成共识，提出"国际人道法只适用于武装冲突局势。专家组回顾了现有国际法原则，包括 2015 年报告中提及的人道原则、必要性原则和比例原则（如适用）。专家组认识到有必要开展进一步研究，明确各国何时以及如何将这些原则适用于信通技术的使用，并强调回顾这些原则绝不是对冲突的合法化或鼓励冲突。"[3]2021-2025 年信息和通信技术安全和使用问题不限成员名额工作组在其报告中也对这一结论表示赞同。[4]

[1] *Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 2021, para. 71(f). Also see United Nations General Assembly Resolution 76/19, 2021, paras 2 and 3, adopted by consensus, which welcomes the consensus final report of the GGE and calls upon member states to be guided in their use of ICTs by the report.

[2] See Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, *First Annual Progress Report*, A/77/275, 2022, para. 15(b)(ii); *Second Annual Progress Report*, A/78/265, 2023, para. 29(b)(ii); *Third Annual Progress Report*, A/79/214, 2024, para. 36(b)(ii); *Draft Final Report,* A/AC.292/2025/CRP.1, 2025, para. 40(b)(ii).

[3] 《从国际安全角度促进网络空间负责任国家行为政府专家组的报告》，A/76/135，2021 年，第 71（f）段。另见联合国大会 2021 年第 76/19 号决议第 2 段和第 3 段，该决议得到一致通过，欢迎政府专家组的协商一致最后报告，并呼吁成员国在使用信通技术时使用该报告。

[4] 见信息和通信技术安全和使用问题不限成员名额工作组（OEWG），《第一次年度进展报告》，A/77/275，2022 年，第 15（b）（ii）段；《第二次年度进展报告》，A/78/265，2023 年，第 29（b）（ii）段；《第三次年度进展报告》，A/79/214，2024 年，第 36（b）（ii）段；《最后报告》，A/AC.292/2025/CRP.1，2025 年，第 40（b）（ii）段。

To date, and to our knowledge, 35 states have published individual national positions on how international law applies to cyber operations. [5] In addition, two regional organizations – the African Union and the European Union – published common positions or understandings on the application of international law to the use of ICTs, marking progress in building regional consensus and bringing the number of states opining on this subject to over 100. Emerging shared understandings include reaffirming the application of IHL principles and rules, including humanity, necessity, proportionality and distinction, to the use of ICTs during armed conflict. A growing number of states have also expressed their views on the protection afforded by IHL for, among others, civilians, civilian infrastructure, civilian data, medical personnel and facilities, and humanitarian activities and personnel against malicious ICT activities.	迄今为止，据我们所知，已有 35 个国家就国际法如何适用于网络行动的问题发布了各自的国家立场。[6] 此外，非洲联盟和欧洲联盟这两大区域性组织也就国际法适用于信通技术的使用这一问题发布了共同立场或共识，标志着在凝聚区域共识方面的进展，并表明已有 100 多个国家就这一主题发表观点。逐渐形成的共识包括重申国际人道法原则和规则，包括人道原则、必要性原则、比例原则和区分原则，在武装冲突期间适用于信通技术的使用。对于国际人道法保护平民、民用基础设施、民用数据、医务人员和医疗机构以及人道行动和人道工作者免受恶意信通技术活动的影响，越来越多的国家也发表了各自观点。
Building on this momentum, in October 2024 the 34th International Conference of the Red Cross and Red Crescent (34IC) – which brought together all states and all components of the International Red Cross and Red Crescent Movement (Movement) – adopted the resolution "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (ICT Resolution). The resolution urges states and parties to armed conflicts to protect the civilian population and other protected persons and objects in situations of armed conflict, including against the risks arising from malicious ICT activities. It also calls on states and parties to armed conflicts to uphold IHL protections for civilians, civilian critical infrastructure (including critical digital infrastructure, such as undersea cables and orbit communication networks), medical and humanitarian personnel and activities, and cultural property, including against the risks arising from ICT activities.	借助这一势头，2024 年 10 月举行的第 34 届红十字与红新月国际大会（简称"第 34 届国际大会"）——汇集了所有国家以及红十字与红新月运动（简称"运动"）各组成部分——通过了"在武装冲突期间保护平民和其他受保护人员及物体免受信息和通信技术活动的潜在人道代价之影响"决议（简称"信通技术决议"）。这一决议敦促各国和武装冲突各方在武装冲突局势中保护平民居民和其他受保护人员和物体，包括免受恶意信通技术活动所带来风险的影响。决议还呼吁各国和武装冲突各方维护国际人道法为平民、关键民用基础设施（包括如海底电缆和轨道通信网络等关键数字基础设施）、医务人员和人道工作者、医疗活动和人道行动以及文化财产所提供的保护，包括保护其免受信通技术活动所带来的风险的影响。决议重申禁止鼓励或煽动违反国际人道法的行为，并讨论了与武装冲突中平民开展信通技术活动以及私营技术公司提供信通技术服务相关的问题。

[5] All individual national positions and common positions can be found at Cyber Law Toolkit, "Common and National Positions", at https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.
[6] 各国具体立场和共同立场的所有文件均收录于"网络法工具包"中关于"国家立场和共同立场"的部分，载：https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions。

It reiterates the prohibition on encouraging or inciting violations of IHL, and addresses issues relating to civilians conducting ICT activities, and private technology companies providing ICT services in the context of armed conflict.	
Despite the progress noted above, it has been recognized that the specificities of the ICT environment raise questions on how principles and rules of IHL apply to ICT activities and that there is a need for further discussions.[7]	虽然已经取得了上述成就，但是各国都认识到，信通技术环境的特性引发了关于国际人道法原则和规则如何适用于信通技术活动的问题，并且有必要就此展开进一步讨论。[8]
This workstream responds to this need and provides a dedicated space for focused and in-depth exchanges. In light of the human cost of the use of ICTs in armed conflict, the objective of the workstream is to foster shared understandings on the limits that IHL imposes on ICT activities in armed conflict to safeguard civilians from harm.	本工作领域对此需求做出回应，并提供了专门空间进行集中深入的交流。鉴于武装冲突中使用信通技术所带来的人道代价，本工作领域旨在就国际人道法在武装冲突中限制信通技术活动这一议题促成共识，从而保护平民居民免受伤害。
II. THE USE OF ICTS IN TODAY'S ARMED CONFLICTS AND THE HUMAN COST	**二、当今武装冲突中信通技术的使用及其人道代价**
The rapid digitalization of societies has brought significant benefits, enhancing social, economic and communication opportunities. In conflict-affected areas, reliable ICTs are critical for civilians to access essential goods and services, for governments to provide services, and for supporting medical and humanitarian activities, including those of the International Red Cross and Red Crescent Movement.	社会的快速数字化带来了诸多积极影响，在社会、经济和通信层面创造了更多机会。在受冲突影响地区，可靠的信通技术能够发挥至关重要的作用，帮助平民获得基本物资和服务，协助政府提供服务，并为包括红十字与红新月运动在内的医疗活动和人道行动提供支持。
However, these advantages also come with risks, including those arising from an increase in the use of ICTs by states and	然而，这些优势同时也伴随着风险，包括武装冲突中各国和非国家行为方日益频繁地使用信通技术所带来的风险。若干国家正在发展用于军事用途的信

[7] *Report of Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, A/76/135, 2021, para. 71(f), and 34th International Conference of the Red Cross and Red Crescent, Geneva, 2024, Resolution 2, "Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict" (hereinafter ICT Resolution), preambular paragraph 19.

[8] 《从国际安全角度促进网络空间负责任国家行为政府专家组的报告》，A/76/135，2021 年，第 71（f）段，以及第 34 届红十字与红新月国际大会，日内瓦，2024 年，第 2 号决议，"在武装冲突期间保护平民和其他受保护人员及物体免受信息和通信技术活动的潜在人道代价之影响"（以下简称"信通技术决议"），序言部分第 19 段。

non-state actors in armed conflicts. A number of states are developing ICT capabilities for military purposes, with growing deployment and use of ICTs as means or methods of warfare. Whereas the development and use of military ICT capabilities may offer belligerents the possibility of achieving their objectives without necessarily causing direct harm to civilians or physical damage to civilian infrastructure, the risk such activities pose to civilian populations and infrastructure remains a real concern. By using military ICT capabilities, processes controlled by computer systems can be triggered, altered or otherwise manipulated with the potential to cause significant harmful effects for civilians.	通技术能力，信通技术日益广泛地作为作战手段和方法进行部署和使用。虽然发展和使用军用信通技术能力有助于交战各方在不必然对平民造成直接伤害或对民用基础设施造成实际损害的情况下实现其目标，但是此类活动为平民居民和基础设施带来的风险仍是一项切实关切。运用军用信通技术能力能够触发、篡改乃至操纵由计算机系统控制的流程，可能会对平民造成严重的不利影响。
The use of ICTs targeting civilian critical infrastructure – such as nuclear facilities, power grids, water systems and telecommunications networks – can have "potentially devastating humanitarian consequences". [9] ICT activities can also disrupt e-governance services and private sector operations, with societal and economic costs. These risks are compounded by the interconnectivity that characterizes cyberspace. ICT activities targeted at one system may have repercussions for various other systems, regardless of where those systems are located.	使用信通技术攻击关键民用基础设施——例如核设施、电网、供水系统和电信网络——可能会产生"潜在的破坏性人道后果"。[10]信通技术活动还可能扰乱数字治理服务和私营领域的运营，继而造成社会和经济损失。并且，网络空间的互联互通性特点会加剧上述风险。攻击某一系统的信通技术活动还可能波及其他诸多系统，不论这些系统位于何处。
The health-care sector, along with humanitarian organizations, is especially vulnerable to ICT activities in armed conflict, which can disrupt life-saving medical operations, impair the operation of impartial humanitarian organizations and their personnel, and jeopardize the provision of essential assistance to those in need. For instance, the International Committee of the Red Cross (ICRC) and	医疗部门和人道组织在武装冲突中尤其容易受到信通技术活动的影响，这类活动可能会中断挽救生命的医疗行动，阻碍公正人道组织及其工作人员的行动，并危及向有需要的人群提供的基本援助。例如，红十字国际委员会以及运动的其他组成部分，均曾受到过信通技术活动的攻击。[12]

[9] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, *Final Substantive Report*, A/AC.290/2021/CRP.2, 2021, para. 18.

[10] 从国际安全角度看信息和电信领域的发展不限成员名额工作组，《最后实务报告》，A/AC.290/2021/CRP.2，2021 年，第 18 段。

[12] 2022 年的数据泄露事件和红十字国际委员会网站重复遭到分布式拒绝服务攻击，突出强调有必要建立强有力的数据保护机制，从而保障敏感信息的安全，确保行动持续性，并保护与冲突各方进行的保密人道对话。见红十字国际委员会，"关于红十字国际委员会遭遇网络攻击事件的当前状况"，载：https://www.icrc.org/zh/document/cyber-attack-icrc-what-we-know。

other components of the Movement, have been targeted by ICT activities.[11]	
Additionally, the involvement of civilians in military activities through the use of ICTs during armed conflict has become more pronounced. States have tolerated, facilitated or encouraged civilian hackers and hacker groups to engage in ICT activities, targeting or affecting civilians and civilian objects associated with the adversary. Civilians have also been encouraged to report enemy troop movements, including via smartphone applications. Private companies are increasingly providing cybersecurity or other digital services to parties to armed conflict. If civilians are drawn closer to hostilities, they risk being exposed to harm. In addition, they are often not aware of the risks they are taking, the legal implications of their activities, or the IHL rules they have to respect.	此外，武装冲突期间平民使用信通技术参与军事活动的情况也愈发显著。各国容忍、便利或鼓励平民黑客参与信通技术活动，攻击或影响与敌方相关联的平民与民用物体。平民还被鼓励报告敌方部队的动向，包括通过智能手机应用程序。私营企业为武装冲突各方提供网络安全或其他数字服务的情况也在日益增多。如果平民被卷入敌对行动，他们将面临受到伤害的风险。此外，他们往往不了解自己所承担的风险，自身行为的法律影响，不了解应遵守的国际人道法规则。
Another dimension is the use of ICTs for spreading harmful information during armed conflict. While information operations have long been part of warfare and are not unlawful as such, the use of ICTs – especially on social media platforms or when coupled with artificial intelligence and other emerging technologies – amplifies the speed and scale of the spread of harmful information, including efforts to incite violence, expose detainees to public curiosity or undermine trust in humanitarian organizations.	武装冲突期间使用信通技术传播有害信息是另一大问题。虽然信息行动早已在战争中开展，本身并不违法，但信通技术的使用——尤其是在社交媒体上，或与人工智能和其他新型技术相结合使用时——加剧了有害信息的传播速度和规模，这些信息涉及煽动暴力、将被拘留者暴露于公众好奇心之下或破坏对人道组织的信任。
States have acknowledged these developments and risks. The OEWG 2021-2025 has noted that states are developing ICT capabilities for military purposes, that the use of ICTs in conflicts is increasingly likely, and that ICTs have already been used in conflicts in different regions, with potentially devastating humanitarian consequences for civilians and civilian objects, as well as for international and	各国已经认识到上述情况和风险。2021-2025 年不限成员名额工作组注意到，各国正在发展军用信通技术能力，在冲突中使用信通技术的可能性日益增加，且不同地区的冲突中已经出现使用信通技术的情况，这可能会带来破坏性的人道后果，对平民和民用物体以及国际组织和人道组织造成重大损害。[15] 第 34 届国际大会也强调了武装冲突各方使用信通技术对平民造成的潜在伤害，尤其是这些手段直接针对关键民用基础设施和基本服务或附带对其造成损

[11] The 2022 data breach and repeated distributed denial-of-service attacks on the ICRC website highlight the need for robust data protection to safeguard sensitive information, ensure operational continuity and protect confidential humanitarian dialogue with parties to conflicts. See ICRC, "Cyber attack on ICRC: What we know", at https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

[15] 信息和通信技术安全和使用问题不限成员名额工作组，《最后报告草案》，A/AC.292/2025/CRP.1，2025 年，第 15、16 和 21 段。

humanitarian organizations.[13] The 34IC has also highlighted the potential harm to civilians caused by the use of ICTs by parties to armed conflicts, particularly where these means are directed against or incidentally affect civilian critical infrastructure and essential services, and the potential harm to impartial humanitarian organizations, hindering these organizations' access to affected populations.[14]	害，以及对公正的人道组织造成的潜在伤害，阻碍了这些组织为受影响民众提供援助。[16]
III. THE USE OF ICTS IN ARMED CONFLICTS: FRAMING THE LEGAL AND HUMANITARIAN QUESTIONS UNDER IHL	**三、武装冲突中信通技术的使用：确定国际人道法下的法律和人道问题**
Existing IHL treaties and customary law provide protection for civilians and civilian objects against the dangers arising from ICT activities during armed conflict. As reiterated by the ICT Resolution, "in situations of armed conflict, IHL rules and principles – including the principle of distinction, the prohibition of indiscriminate and disproportionate attacks, the obligations to spare the civilian population, civilians and civilian objects in the conduct of military operations, and to take all feasible precautions to avoid, and in any event minimize, incidental civilian harm, the prohibition of encouraging or inciting violations of IHL, and the prohibition of acts or threats of violence, the primary purpose of which is to spread terror among the civilian population – serve to protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities".[17]	现有的国际人道法条约和习惯法，为武装冲突期间平民和民用物体免受信通技术活动所带来的危害提供了保护。正如信通技术决议所重申的："在武装冲突局势中，国际人道法规则和原则——包括区分原则，禁止不分皂白及不成比例的攻击，在军事行动中避免伤害平民居民、平民和民用物体的义务以及采取一切可行的预防措施以避免并尽量减少对平民的附带损害的义务，禁止鼓励或煽动违反国际人道法的行为，以及禁止主要旨在向平民居民散布恐怖的暴力行为或暴力威胁——为平民居民和其他受保护人员和物体提供保护，包括免受信通技术活动所带来的风险。"[18]
Building on the above, the key legal issues below, relating to the most pressing humanitarian concerns, are proposed for further discussion.	基于以上内容，我们提出了如下事关最迫切之人道关切的关键性法律问题，供进一步讨论。

[13] Open-ended Working Group on Security of and in the Use of Information and Communications Technologies, *Draft Final Report,* A/AC.292/2025/CRP.1, 2025, paras. 15, 16 and 21.
[14] ICT Resolution, preambular paras 7 and 14.
[16] 信通技术决议，序言部分第 7 段和第 14 段。
[17] ICT Resolution, para. 4.
[18] 信通技术决议，第 4 段。

I.PROTECTING CIVILIANS AND OTHER PROTECTED PERSONS AND OBJECTS FROM THE DANGERS ARISING FROM ICT ACTIVITIES DURING ARMED CONFLICTS	**（一）武装冲突期间保护平民和其他受保护人员及物体免受信通技术活动所带来的危害**
Protecting civilian populations from the effects of ICT operations during armed conflicts and the notion of attack under IHL	**保护平民居民免受武装冲突期间信通技术行动的影响以及国际人道法中对攻击的界定**
ICT operations have the potential to disable or physically damage industrial facilities, communication networks and other elements of a state's critical infrastructure. Such operations can also directly or indirectly cause injury or death to civilians – including by disrupting the functioning of essential services. These risks are compounded by the interconnectivity of digital space. While ICT operations that result in physical damage have received specific attention, the recent uses of ICTs, including in armed conflicts, have shown that even in the absence of physical damage, ICT operations can severely disrupt civilian infrastructure and interrupt the delivery of essential services. In fact, this constitutes one of the most important ICT risks for civilians during armed conflict.	信通技术行动可能会致使一国关键基础设施中的工业设施、通信网络和其他部分失去效用或受到实际损害。此类行动也可能会直接或间接地造成平民伤亡，包括通过扰乱基本服务的正常运作。网络空间的互联互通性特点还会加剧这些风险。虽然造成物理损害的信通技术行动已得到特别关注，但是近期信通技术在武装冲突等情况下的使用，表明即使未造成物理损害，此类行动也会严重扰乱民用基础设施并中断基本服务的供应。实际上，这正是武装冲突期间信通技术对平民造成的最重要风险之一。
The purpose of the IHL rules governing the conduct of hostilities is to ensure respect for and protection of the civilian population and civilian objects.[19] Most rules stemming from the principles and rules governing the conduct of hostilities, notably distinction, proportionality and precautions – which provide general protection for civilians and civilian objects – apply only to operations or activities that qualify as "attacks", as defined in IHL, i.e. "acts of violence against the adversary, whether in offence or in defence".[20] The question of how the notion of "attack" is interpreted with regard to the use of ICTs during armed conflict, in particular to ICT operations that disable civilian objects without causing physical damage, is therefore essential, as this	规制敌对行动的国际人道法规则旨在确保对平民居民和民用物体的尊重并为之提供保护。[21]源于规制敌对行动原则和规则的大多数规则，特别是为平民和民用物体提供一般保护的区分原则、比例原则和预防措施原则仅适用于根据国际人道法的定义构成"攻击"的行动或活动，即"不论在进攻或防御中对敌人的暴力行为"。[22]因此，在武装冲突期间使用信通技术，尤其是在致使民用物体失去效用而未造成物理损害的信通技术行动中，对"攻击"这一概念的解释问题至关重要，因为这将决定上述规则能否适用，从而决定平民和其他受保护人员和物体是否能受到保护，免受此类行动所带来的危害。

[19] Additional Protocol I of 8 June 1977, Article 48 and titles of Part IV and Section I.
[20] Additional Protocol I, Article 49(1). There are a few IHL rules that apply to all military operations, including those carried out through ICT activities. See, for example, Additional Protocol I, Articles 48, 51(1) and 57(1).
[21] 1977 年 6 月 8 日《第一附加议定书》第 48 条和第四部标题及第一编。
[22] 《第一附加议定书》第 49 条第 1 款。一些国际人道法规则适用于所有军事行动，包括通过信通技术进行的军事活动，例如，见《第一附加议定书》第 48 条、第 51 条第 1 款和第 57 条第 1 款。

determines whether these rules apply, and thus whether civilians and other protected persons and objects are protected against the dangers arising from such operations.	
It is well established that the notion of violence in the definition of "attack" under IHL can refer to either the means used or the consequences or effects produced. An operation that causes violent effects qualifies as an attack, even if the means used are not violent in themselves.[23]	现在公认的是，在国际人道法对"攻击"的定义中，暴力这一概念既可以指所使用的手段，也可以指所造成的后果或影响。某一行动即便使用的手段本身不具暴力性质，但只要造成暴力影响，该行动就构成攻击。[24]
It is also widely accepted that an ICT operation that is expected to cause death or injury to a person, or damage or destruction to an object, constitutes an attack under IHL.[25] It is commonly understood that this includes harm due to the foreseeable direct and indirect (or reverberating) effects of an operation, for example the death of patients in intensive-care units caused by an ICT operation against an electricity network that results in cutting off a hospital's power supply.[26]	同样得到广泛接受的是，凡是预期会造成人员伤亡，或者造成物体损害或毁坏的信通技术行动均构成国际人道法下的攻击。[27]人们普遍认为，这包括某一行动可预见的直接和间接（或衍生）影响所带来的伤害，例如：针对供电网络的信通技术行动导致医院断电，进而造成重症监护病房内患者死亡。[28]
Beyond this, further discussion among states is needed on which IHL rules limit ICT operations that affect the functionality of ICT systems without necessarily causing physical damage or destruction to an object or injury or death to a person, including whether they qualify as "attacks" under IHL.	此外，各国还需进一步讨论，对于影响信通技术系统运转但未必会造成物体物理损害或毁坏或者人员伤亡的信通技术行动，哪些国际人道法规则对其加以限制，包括这些行动是否构成国际人道法下的"攻击"。
From a contemporary warfare perspective, recognizing as an attack under IHL, an ICT	从当代战争角度出发，承认致使某一物体失去效用但未造成物理损害的信通技术行动构成国际人道法

[23] Y. Sandoz, C. Swinarski and B. Zimmermann (eds), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, ICRC, Geneva/Martinus Nijhoff, Leiden, 1987 (hereafter ICRC, Commentary on the Additional Protocols), para. 1881 on Article 49(1) of Additional Protocol I states that "there is an attack whenever a person is directly endangered by a mine laid", which is an interpretation consistent with the consequence-based approach. Another generally accepted example is that the use of a chemical or biological agent would constitute an attack due to the violent effects it causes, even if the means of delivering such agents may not be violent.

[24] 伊夫·桑多，克里斯托夫·斯维纳尔斯基，布鲁诺·齐默尔曼（编），《1949 年 8 月 12 日日内瓦四公约之 1977 年 6 月 8 日附加议定书的评注》，日内瓦/马蒂纳斯·奈霍夫，莱顿，1987 年（以下简称"红十字国际委员会，《〈附加议定书〉评注》"），关于《第一附加议定书》第 49 条第 1 款的评注第 1881 段写道，"只要有任何人直接受到埋放地雷（水雷）的危害，就存在攻击"，这一解释和以后果为基础的解释方法相一致。另一个普遍接受的示例是，使用化学或生物制剂会因其造成的暴力影响而构成攻击，即使投送这些制剂的手段并不具有暴力性。

[25] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2015, pp. 41–42.

[26] ICRC, *Position Paper on International Humanitarian Law and Cyber Operations during Armed* Conflicts, 2019, p. 7. For an overview of positions taken by states, see Cyber Law Toolkit, "Attack (International Humanitarian Law)", at https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).

[27] 红十字国际委员会，《国际人道法及其在当代武装冲突中面临的挑战》，2015 年，第 39～40 页。

[28] 红十字国际委员会，《国际人道法与武装冲突中的网络行动立场文件》，2019 年，第 7 页。关于各国立场的概述，见"网络法工具包"中关于"攻击（国际人道法）"的部分，载：https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law)。

operation that disables an object without causing physical damage, is crucial for the protection of civilians and civilian objects against ICT activities during armed conflict. A restrictive interpretation of the notion of attack, that excludes certain ICT activities from the protection afforded by key IHL rules on the conduct of hostilities, would be difficult to reconcile with the object and purpose of IHL, and with the need to ensure that its protective framework remains effective in light of the evolving means and methods of warfare. It is essential in this regard that states find a common understanding to protect civilians and civilian objects against the effects of harmful use of ICTs during armed conflict.	下的攻击行为，对于武装冲突期间保护平民和民用物体免受信通技术活动的危害十分重要。如果对攻击这一概念进行限缩性解释，将某些信通技术活动排除在规制敌对行动的主要国际人道法规则所提供的保护之外，就很难与国际人道法的宗旨和目的相契合，也难以确保其保护性框架面对不断演变的作战手段和方法能够始终有效。在这方面，各国亟需达成共识，在武装冲突期间保护平民和民用物体免受信通技术的使用所带来的危害。
Civilian data and the notion of civilian objects under IHL	**民用数据和国际人道法对民用物体的界定**
Civilian data – such as medical data, biometric data, social security data, tax records, bank accounts, humanitarian data, companies' client files or election lists and records – are an essential component of digitalized societies. Such data are key to the functioning of most aspects of civilian life, be it at the individual or societal level. There is increasing concern about protecting such data. Deleting or tampering with civilian data can quickly bring government services and private businesses to a standstill and may cause more harm to civilians than the destruction of certain physical objects. In addition, stealing or leaking civilian data can expose individuals and communities to serious risks of harm.	民用数据——例如医疗数据、生物识别数据、社会保障数据、税务记录、银行账户、人道数据、企业客户档案或选举名单和记录——是数字化社会的基本组成部分。这些数据对于个人或社会层面的大部分民生运转都至关重要。如何保护这些数据越发令人关切。删除或篡改民用数据可能会迅速造成政府服务和私营企业停摆，甚至比摧毁某些物理实体对平民的造成伤害更为严重。此外，窃取或泄露民用数据会使个人和社区面临严重的伤害风险。
With regard to data belonging to certain categories of persons and objects that enjoy specific protection under IHL, the protective rules are comprehensive. For example, the obligation to respect and protect medical personnel, units and transports, humanitarian personnel and objects, and objects indispensable for the survival of the	对于受到国际人道法特别保护的特定类别人员和物体的数据，相关的保护性规则是全面的。例如，尊重和保护医务人员与医疗队和医务运输工具、人道工作者和物资、对平民居民生存所不可缺少的物体的义务，同样适用于他们的数据。[31]但除此之外，更深入地理解现有国际人道法规则[32]对民用数据的保护程度也很重要，尤其是数据是否构成国际人道法所规定的物体。如果构成的话，则针对数据的信通技

[31] 见本文件下一小节，“依据国际人道法受到特别保护的人员和物体”。
[32] 这些规则包括有关敌对行动的国际人道法规则和原则。其他相关规则可能包括，保护文化财产、保护财产免遭扣押和毁坏，以及禁止掠夺。

civilian population extend to their data.[29] Beyond that, however, it is important to better understand the extent to which civilian data are protected by existing IHL rules, [30] in particular whether data constitute objects as understood under IHL, in which case ICT operations against data (such as damaging or deleting them) would notably be governed by the principles of distinction, proportionality and precaution.	术行动（损坏或删除数据）将主要受到区分原则、比例原则和预防措施原则的规制。
In this respect, some states have taken the view that the protection of civilian objects extends to all types of civilian data; some seem to draw a difference between "content data" and other data; while others have taken the view that digital data cannot generally be considered to be objects under IHL.[33]	在此方面，一些国家认为对民用物体的保护扩展适用于所有类型的民用数据；一些国家似乎对"内容数据"和其他数据进行了区分；而另一些国家认为数字数据通常不能视作国际人道法下的物体。[34]
Further discussion among states is needed to build shared understandings on this critical issue. From a humanitarian perspective, the assertion that an operation designed or expected to delete or tamper with civilian data would not be prohibited by IHL in today's data-reliant world seems difficult to reconcile with the object and purpose of IHL. Logically, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to the information stored in the data.	各国需要进一步讨论，就这一关键问题达成共识。从人道角度出发，在当前依赖数据的世界，旨在或预计会删除或篡改民用数据的行动不受国际人道法禁止这一主张，似乎很难与国际人道法的宗旨和目的相契合。就逻辑而言，用数据形式的数字档案取代纸质档案和文件，不应降低国际人道法对数据中存储信息的保护力度。
Specific protections for persons, objects and activities under IHL	**依据国际人道法受到特别保护的人员、物体及活动**
Some rules of IHL afford specific protection to certain categories of persons, objects and activities, beyond the prohibition of attacks, including with regard to ICT activities.	一些国际人道法规则为特定类别的人员、物体及活动提供了除禁止攻击之外的特别保护，这也包括涉及信通技术活动。

[29] See the next section of this paper, "Specifically protected persons and objects under IHL".
[30] These include IHL principles and rules on the conduct of hostilities. Other relevant rules may include the protection of cultural property, the protection of property against seizure and destruction, and the prohibition of pillage.
[33] For an overview of positions taken by states, see Cyber Law Toolkit, "Data as a military objective", at https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.
[34] 关于各国立场概述，见"网络法工具包"中关于"作为军事目标的数据"的部分，载：https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL。

For example, belligerents must respect and protect medical personnel and facilities at all times,[35] including the requirement not to unduly interfere with the functioning of medical services and take feasible measures to protect them against harm or interferences from private persons not attributable to parties to armed conflict.[36] Likewise, humanitarian personnel and objects used for humanitarian operations must be respected and protected; [37] and parties to armed conflicts must allow and facilitate impartial humanitarian activities during armed conflict subject to their right of control.[38] For both medical services and humanitarian personnel and objects, specific protection extends to communications and data.[39]	例如，交战各方必须始终尊重和保护医务人员和医疗设施，[40]这包括不得不当干扰医疗服务的运作，并采取可行措施保护他们免受非武装冲突各方的私人造成的伤害或干扰。[41]与之类似，人道工作者和用于人道行动的物体必须得到尊重和保护；[42]武装冲突各方必须在其控制权内允许进行公正的人道活动并为之提供便利。[43]对医疗服务以及人道工作者和物资而言，特别保护扩展适用于相关通信和数据。[44]
To strengthen the protection of medical services and humanitarian activities against ICT-related risks, further discussion may focus on how to operationalize such protection. One avenue is the effort led by the ICRC to develop a digital emblem – that is, a means of identifying the digital infrastructure and data of organizations and entities entitled to display the distinctive emblems recognized under IHL.[45] The ICT Resolution, taking note of the ongoing work of the ICRC in consultation with states and components of the Movement, encourages	为加强对医疗服务和人道活动的保护，使其免受信通技术相关风险的影响，进一步讨论时可重点关注如何落实此种保护。途径之一是红十字国际委员会主导的一项开发数字标志的工作。数字标志是针对有权展示国际人道法所规定的特殊标志的组织和实体，可以识别其数字基础设施和数据的一种手段。[47]“信通技术决议”注意到红十字国际委员会经与各国和运动的组成部分进行咨商而开展的当前工作，鼓励展开进一步工作与咨商，包括研究数字标志的潜在用途方面可能的法律和外交渠道。[48]

[35] See, for instance, First Geneva Convention of 12 August 1949, Article 19; Second Geneva Convention of 12 August 1949, Article 12; Fourth Geneva Convention of 12 August 1949, Article 18; Additional Protocol I, Article 12; Additional Protocol II of 8 June 1977, Article 11; ICRC, Customary IHL Study, at https://ihl-databases.icrc.org/en/customary-ihl/rules (hereafter ICRC, Customary IHL Study), Rules 25, 28 and 29.

[36] ICRC, Commentary on the Additional Protocols, para. 517 on Article 12 of Additional Protocol I, and ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, 2nd ed., ICRC, Geneva / Cambridge University, Cambridge, 2016 (hereafter ICRC, Commentary on the First Geneva Convention, 2016), para. 1799 on Article 19.

[37] Additional Protocol I, Articles 70(4) and 71(2); ICRC, Customary IHL Study, Rules 31 and 32.

[38] See Fourth Geneva Convention, Article 23; Additional Protocol I, Article 70(2); Additional Protocol II, Article 18(2); ICRC, Customary IHL Study, Rules 55.

[39] ICRC, Commentary on the First Geneva Convention, 2016, para. 1804 on Article 19.

[40] 例如，见 1949 年 8 月 12 日《日内瓦第一公约》第 19 条；1949 年 8 月 12 日《日内瓦第二公约》第 12 条；1949 年 8 月 12 日《日内瓦第四公约》第 18 条；《第一附加议定书》第 12 条；1977 年 6 月 8 日《第二附加议定书》第 11 条；红十字国际委员会，《习惯国际人道法研究》，载：https://ihl-databases.icrc.org/zh/customary-ihl/rules（以下简称“红十字国际委员会，《习惯国际人道法研究》”），规则 25、规则 28 和规则 29。

[41] 红十字国际委员会，《附加议定书评注》，《第一附加议定书》第十二条评注第 517 段，以及红十字国际委员会，《〈日内瓦第一公约〉评注：改善战地武装部队伤者病者境遇之日内瓦公约》，第二版，红十字国际委员会，日内瓦/剑桥大学，剑桥，2016 年（以下简称“红十字国际委员会，《〈日内瓦第一公约〉评注》，2016 年”），关于第 19 条的评注，第 1799 段。

[42] 《第一附加议定书》第 70 条第 4 款和第 71 条第 2 款；红十字国际委员会，《习惯国际人道法研究》规则 31 和规则 32。

[43] 见《日内瓦第四公约》第 23 条；《第一附加议定书》第 70 条第 2 款；《第二附加议定书》第 18 条第 2 款；红十字国际委员会，《习惯国际人道法研究》规则 55。

[28] 红十字国际委员会，《〈日内瓦第一公约〉评注》，2016 年，关于第 19 条的评注第 1804 段。

[45] The Digital Emblem project is a stand-alone project led by the ICRC in consultation and engagement with states and components of the Movement. The discussion within this workstream will not focus on this project.

[47] “数字标志”项目是经与各国和国际红十字与红新月运动的组成部分进行咨商和沟通，由红十字国际委员会主导的独立项目。本工作领域将不会重点讨论该项目。

[48] 信通技术决议，序言部分第 15 段和执行部分第 12 段。

further work and consultations, including to study possible legal and diplomatic avenues for the potential use of a digital emblem.[46]	
Furthermore, ICT activities that "destroy, remove or render useless" objects indispensable to the survival of the civilian population, such as drinking water installations and irrigation works, fall within the scope of the special protection accorded to such objects under IHL, irrespective of whether they qualify as attacks.[49] The special protection extends to ICT infrastructure that is itself "indispensable" to the functioning of such objects. Further discussion is needed on measures to operationalize such protections.	此外，对平民居民生存所不可缺少的物体，如饮水装置和灌溉工程，进行"毁坏、移动或使其失去效用"的信通技术活动，无论其是否构成攻击，均属于国际人道法对此类物体所赋予特别保护的范畴。[50] 特别保护还延伸至本身对此类物体的运行"所不可缺少"的信通技术基础设施。需就落实此种保护的措施进行进一步讨论。
Finally, IHL rules prohibit sexual violence and afford specific protections to certain categories of persons, including though not limited to women, elderly, persons with disabilities and children (for instance, against their unlawful recruitment or use in hostilities).[51] Further discussion is needed, among other issues, on practical measures to ensure compliance with these rules, including when facilitated by ICTs.	最后，国际人道法规则禁止性暴力并为特定类别的人员提供了特别保护，包括但不限于妇女、老人、残疾人和儿童（例如禁止在敌对行动中非法征募和使用儿童）。[52]尤需进一步讨论的问题是应采取哪些切实措施确保遵守这些规则，包括信通技术协助的情况下。
II.PROTECTING CIVILIANS AND OTHER PROTECTED PERSONS FROM INFORMATION SPREAD IN VIOLATION OF IHL DURING ARMED CONFLICTS	**（二）武装冲突期间保护平民和其他受保护人员免受违反国际人道法的信息传播活动之害**
States and non-state armed groups are spreading digital information for a variety of purposes, including when carrying out information or psychological operations. Some operations aim to reduce the risk of harm to humans during armed conflicts, for	国家和非国家武装团体（包括在开展信息行动或心理行动时）传播数字信息出于多种目的：有些行动旨在减少武装冲突中对人类造成伤害的风险，例如在攻击之前向平民提前发出有效警告，或帮助指引他们前往安全场所；其他行动则意在造成困惑或伤害、欺骗敌方，或支持冲突一方的军事或政治目

[46] ICT Resolution, preambular para. 15 and operative para. 12.

[49] Examples of such objects include, but are not limited to, "foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works." Additional Protocol I, Article 54(2); Additional Protocol II, Article 14; ICRC, Customary IHL Study, Rule 54. See also ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 46–47.

[50] 例如，此类物体包括但不限于"粮食、生产粮食的农业区、农作物、牲畜、饮水装置和饮水供应和灌溉工程"。《第一附加议定书》第 54 条第 2 款；《第二附加议定书》第 14 条；红十字国际委员会，《习惯国际人道法研究》规则 54。另见红十字国际委员会，《国际人道法及其在当代武装冲突中面临的挑战》，2024 年，第 46～47 页。

[51] Fourth Geneva Convention, Article 27(2); Additional Protocol I, Articles 76(1) and, 77(1) and (2); Additional Protocol II, Article 4(3)(c); ICRC, Customary IHL Study, Rules 134 to138.

[52] 《日内瓦第四公约》第 27 条第 2 款；《第一附加议定书》第 76 条第 1 款和第 77 条第 1 款和第 2 款；《第二附加议定书》第 4 条第 3 款第 3 项；红十字国际委员会，《习惯国际人道法研究》规则 134 至规则 138。

example by giving civilians an effective advance warning of an attack or by helping to direct them to safety. Others are designed to cause confusion or harm, to deceive an adversary or to support the military or political objectives of a party to the conflict. In today's armed conflicts, ICT activities are used to spread information in violation of IHL. Information spread through ICT activities can contribute to or encourage violence, cause lasting psychological harm, undermine access to essential services and disrupt the operations of humanitarian organizations, which may undermine trust in these organizations.	标。在如今的武装冲突中，信通技术活动会用于违反国际人道法的信息传播活动。通过信通技术活动所传播的信息可能会推动或助长暴力、造成长期心理创伤、使民众难以获得基本服务，并破坏人道组织的行动，从而削弱对这些组织的信任。
IHL contains several specific rules that impose limits on spreading information, including through digital means, in particular the following:	国际人道法载有具体规则，对传播信息（包括通过数字手段传播信息）的行为施以限制，尤其是下列规则：
• Civilian and military officials of a party to an armed conflict must not encourage IHL violations, including through digital platforms.[53] The ICT Resolution further reaffirms the prohibition of encouraging or inciting violations of IHL through digital means.[54]	• 武装冲突一方的文职与军事官员不得鼓励违反国际人道法的行为，包括通过数字平台助长。[55]“信通技术决议”进一步重申禁止通过数字手段鼓励或煽动违反国际人道法的行为。[56]
• Prisoners of war and other protected persons under IHL must be protected against public curiosity.[57] Public sharing by authorities of data, images and videos of prisoners of war and others deprived of their liberty, subject to limited exceptions, would violate this rule, and states must protect against sharing by private entities as well.[58]	• 战俘和国际人道法下的其他受保护人员必须得到保护，免受公众好奇心的烦扰。[59]除有限的例外情形外，当局公开分享战俘和其他被剥夺自由者的数据、图像和视频的行为均构成对该条规则的违反，且各国还必须防止私营实体的此等分享行为。[60]
• Threats of violence the primary purpose of which is to spread terror	• 国际人道法禁止以在平民居民中散布恐怖为主要目的的暴力威胁。[62]

[53] Fourth Geneva Convention, Common Article 1; ICRC, Customary IHL Study, Rule 139.
[54] ICT Resolution, para. 4.
[55] 《日内瓦第四公约》共同第 1 条；红十字国际委员会，《习惯国际人道法研究》规则 139。
[56] 信通技术决议，第 4 段。
[57] See, for example, Third Geneva Convention of 12 August 1949, Article 13 and Fourth Geneva Convention, Article 27.
[58] For further discussion on this issue, see, for example, ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War, 2nd ed.*, ICRC, Geneva, 2020 (hereafter ICRC, Commentary on the Third Geneva Convention, 2020), paras 1623–1632.
[59] 例如，见 1949 年 8 月 12 日《日内瓦第三公约》第 13 条和《日内瓦第四公约》第 27 条。
[60] 关于对这一问题的进一步讨论，例如，见红十字国际委员会，《〈日内瓦第三公约〉评注：关于战俘待遇之日内瓦公约》，第二版，红十字国际委员会，日内瓦，2020 年（以下简称“红十字国际委员会，《〈日内瓦第三公约〉评注》，2020 年”），第 1623~1632 段。
[62] 《第一附加议定书》第 51 条第 2 款；《第二附加议定书》第 13 条第 2 款；红十字国际委员会，《习惯国际人道法研究》规则 2。

among the civilian population are prohibited under IHL.[61]	
• False information spread by parties to armed conflict to obstruct medical or humanitarian work is incompatible with the obligations to respect and protect medical and humanitarian personnel and their activities.[63]	• 武装冲突各方传播虚假信息以阻碍医疗或人道工作的行为，与尊重并保护医务人员、人道工作者及其所开展活动的义务是不相容的。[64]
• Information spread for the purpose of child recruitment, or propaganda aimed at enlisting protected persons in occupied territories, into the armed forces is unlawful.[65]	• 以征募儿童兵为目的的信息传播活动，或以征募被占领土的受保护人员加入武装部队为目的的宣传活动是非法的。[66]
Given the above-mentioned risks of harm for civilians and other protected persons under IHL, further discussion is needed to develop shared understandings on how IHL applies to information spread, ensuring the effective protection of all protected persons and objects under IHL.	鉴于上述平民和国际人道法下的其他受保护人员所面临的伤害风险，需要进一步讨论以就国际人道法如何适用于信息传播形成共识，从而确保有效保护国际人道法下的所有受保护人员和物体。
III.THE RISK OF HARM ARISING FROM THE MILITARY USE OF CIVILIAN ICT INFRASTRUCTURE AND THE INVOLVEMENT OF CIVILIANS IN ICT ACTIVITIES DURING ARMED CONFLICTS	**（三）军方使用民用信通技术基础设施以及平民在武装冲突中参与信通技术活动可能导致的伤害风险**
The military use of civilian ICT infrastructure and the resulting impact on its protection under IHL	**军方使用民用信通技术基础设施及其对国际人道法赋予此类设施的保护造成的影响**
Except for certain military networks, cyberspace is predominantly civilian. However, the interconnectedness of civilian and military networks and the use of civilian ICT infrastructure by the military pose specific challenges for its protection.	除特定军用网络外，网络空间主要为民用性质。然而，军民网络的互联互通以及军方使用民用信通技术基础设施的行为对此类设施的保护造成了特殊挑战。
If civilian ICT infrastructure – including infrastructure provided by technology companies – is used for military purposes (in which case such infrastructure is	如果民用信通技术基础设施（包括技术公司提供的基础设施）用于军事目的（在这种情况下，此类基础设施有时会被称为“军民两用”基础设施），则有可能会成为国际人道法意义上的军事目标，并丧

[61] Additional Protocol I, Article 51(2); Additional Protocol II, Article 13(2); ICRC, Customary IHL Study, Rule 2.
[63] This, of course, is different from criticism or the expression of anger by authorities or beneficiaries directed at the medical services or humanitarian organizations, which is not *prima facie* unlawful.
[64] 当然，这不同于当局或受益人针对医疗服务或人道组织进行批评或表达愤怒的行为，后者表面上并不构成违法。
[65] Regarding child recruitment, see ICRC, Customary IHL Study, Rule 136 and obligations under the Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict of 25 May 2000. Regarding protected persons in situations of occupation, see Fourth Geneva Convention, Article 51.
[66] 关于招募儿童问题，见红十字国际委员会，《习惯国际人道法研究》规则 136，和 2000 年 5 月 25 日《〈儿童权利公约〉关于儿童卷入武装冲突问题的任择议定书》所规定的义务。关于占领局势下的受保护人员，见《日内瓦第四公约》第 51 条。

sometimes referred to as "dual-use"), it risks becoming a military objective under IHL and losing its protection against attack.[67] In such cases, civilians and civilian objects in physical proximity, digitally connected to or dependent on such infrastructure, risk incidental harm.	失免受攻击的保护。[68]此时，邻近此类设施、通过数字手段与其相连，或依赖于此类设施的平民和民用物体都可能会受到附带伤害。
However, not every military use turns a civilian object into a military objective under IHL; this occurs only when the use meets the criteria for a military objective as defined by IHL. Furthermore, even if a belligerent considers a civilian or civilian object to have lost protection due to involvement in ICT operations, any attack remains subject to the prohibitions on indiscriminate and disproportionate attacks and the obligation to take all feasible precautions. Additionally, certain specifically protected objects may not be attacked or may be subject to stricter limitations, even when they fulfil the definition of a military objective.	然而，并非只要军方使用了民用物体，就会使其变为国际人道法意义上的军事目标；只有在此种使用行为满足国际人道法对军事目标定义的标准时方可导致转变。此外，即使交战方认为某平民或民用物体由于参与了信通技术行动而丧失了保护，任何攻击也仍要遵守禁止不分皂白和不成比例的攻击的规定，以及采取一切可行的预防措施的义务。而且，某些受到特别保护的物体即使符合军事目标的定义，可能也不得予以攻击，或可能受更严格的限制条件的约束。
To protect civilian populations and essential civilian services relying on ICT infrastructure, further discussion is necessary to determine when military use of predominantly civilian ICT infrastructure turns it into a military objective, and to identify and implement other feasible protective measures. For instance, the ICRC has called on states to, whenever feasible, segment – that is physically or technically separate – ICT infrastructure (or parts thereof) used for military purposes from that used for civilian purposes.[69] It is also essential to ensure that any specific protection granted under IHL is respected.	为保护依赖于信通技术基础设施的平民居民和基本民用服务，有必要开展进一步讨论，以判断军事使用在何种条件下会将主要为民用性质的信通技术基础设施变为军事目标，并明确、实施其他可行的保护性措施。例如，红十字国际委员会呼吁各国在可行的情况下，将用于军事用途与用于民用目的信通技术基础设施（或其部分）——在物理层面或技术层面——分割开来。[70]另外，还必须确保国际人道法所规定的任何特别保护均得到尊重。

[67] Dual-use objects may become military objectives if they, under the circumstances ruling at the time, fulfil the definition under Article 52(2) of Additional Protocol I: "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage".

[68] 军民两用物体如果在当时情况下满足《第一附加议定书》第 52 条第 2 款对军事目标的定义，则有可能成为军事目标。该款规定："就物体而言，军事目标只限于由于其性质、位置、目的或用途对军事行动有实际贡献，而且在当时情况下其全部或部分毁坏、缴获或失去效用提供明确的军事利益的物体"。

[69] One example would be when deciding whether to store military data on a non-segmented commercial cloud, a segment of a commercial cloud or dedicated military digital infrastructure, military planners and operators should not use the non-segmented commercial cloud. See ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2024, pp. 53–54.

[70] 例如，在决定将军事数据是存储在无分区式商业云、商业云的一个分区还是军事专用数字基础设施上时，军事规划人员和操作人员不应使用无分区式商业云。见红十字国际委员会，《国际人道法及其在当代武装冲突中面临的挑战》，2024 年，第 60 页。

The involvement of civilians in ICT activities during armed conflicts	**平民在武装冲突中参与信通技术活动**
In today's armed conflicts, several trends pose risks for civilians: civilian hackers increasingly target civilian objects in ICT operations; parties to armed conflict encourage civilians to collect militarily relevant information through digital means, exposing them to attacks; and civilian technology companies providing ICT services and infrastructure to armed forces risk losing their legal protection.	在当今武装冲突中，有几种趋势对平民构成风险：平民黑客在信通技术行动中越来越多地以民用物体为目标；武装冲突各方鼓动平民通过数字手段收集军事相关信息，使其可能遭受攻击；以及平民技术公司为武装部队提供信通技术服务与基础设施，并因而可能丧失法律保护。
IHL is built on the cardinal principle of distinction. The growing civilian involvement in ICT operations and the military use of civilian ICT infrastructure risk undermining the protection that this foundational principle is meant to provide to civilians, including against being misidentified as lawful targets.	国际人道法以区分原则这一重要原则为基石。平民日益参与信通技术行动，加之军方使用民用信通技术基础设施，有可能会削弱这一根本原则意在为平民提供的保护，包括保护他们不被误认为是合法目标。
Individuals and groups, including hackers and technology company employees, conducting ICT activities in the context of armed conflicts must comply with the limits that IHL sets for such activities,[71] and be aware of the risks involved. In exceptional cases, civilian involvement in ICT activities may amount to "direct participation in hostilities", meaning that a civilian loses the protection against attack for such time only as this is the case. However, in case of doubt, IHL requires that a person be considered civilian and protected as such.[72]	在武装冲突背景下开展信通技术活动的个人和团体，包括黑客与技术公司职员，均须遵守国际人道法针对此类活动施加的限制，[73]并了解所涉及的风险。在特殊情况下，平民参与信通技术活动可能会构成"直接参加敌对行动"，意味着平民仅在直接参加敌对行动时会失去免遭攻击的保护。然而，如对某人的平民身份存疑，国际人道法规定应将该人视为平民并按照平民身份予以保护。[74]

[71] With regard to civilian hackers operating in the context of armed conflicts, these limits have been summarized in ICRC, "Eight rules for 'civilian hackers' during war, and four obligations for states to restrain them", at https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them. On the relevance of IHL to private businesses, see more generally, ICRC, *Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law*, 2024.

[72] Additional Protocol I, Article 50(1). If there is a risk that children may be drawn into hostilities through ICT activities and considered as directly participating in hostilities, belligerents have an additional obligation to prevent the involvement of children under 15 or 18, depending on the applicable legal framework.

[73] 就平民黑客在武装冲突背景下开展行动而言，相关限制归纳总结在以下文件中：红十字国际委员会，"战争中针对'平民黑客'的八条规则以及各国对其予以限制的四项义务"，载：https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them。关于国际人道法对私营企业的相关性，相关总体介绍，见红十字国际委员会，《商业与国际人道法：与企业相关的国际人道法规则简介》，2024 年。

[74] 《第一附加议定书》第 50 条第 1 款。如果存在儿童通过信通技术活动被卷入敌对行动并被视作直接参加敌对行动的风险，则依据适用的法律框架，交战方负有额外义务，须预防 15 岁或 18 岁以下的儿童参与此类活动。

States' responsibility to disseminate IHL and to prevent and suppress IHL violations	国家传播国际人道法并防止和制止违反国际人道法行为的责任
With regard to civilian involvement in ICT activities during armed conflict, it should be noted that states have undertaken to respect and ensure respect for IHL. If civilian hackers, private companies or other private individuals or entities act under the instruction, direction or control of a state, that state is internationally legally responsible for any conduct of those individuals that is inconsistent with the state's international legal obligations, including IHL.[75]	就平民在武装冲突中参与信通技术活动而言，应当指出各国已承诺尊重国际人道法，并确保对国际人道法的尊重。如果平民黑客、私营企业或其他私人个人或实体按照一国的指示或在其指挥或控制下行事，则该国应对这些个人不符合该国国际法律义务（包括国际人道法）的任何行为承担国际法律责任。[76]
Even if the conduct of civilians is not attributable to a party to armed conflict, states are nonetheless obliged to ensure respect for IHL. At a minimum, parties to an armed conflict must not encourage, aid or assist civilians involved in ICT activities to violate IHL,[77] for example by encouraging civilians to direct ICT operations against civilian objects. Furthermore, states must disseminate knowledge of IHL, prevent and suppress violations of IHL, and investigate and prosecute war crimes, including those committed by the civilian population.[78]	即使平民的行为无法归因于武装冲突一方，各国也仍有义务确保对国际人道法的尊重。武装冲突各方至少不得鼓动、援助或协助参与信通技术活动的平民违反国际人道法，[79]例如鼓动平民开展信通技术行动攻击民用物体。此外，各国必须传播国际人道法知识，防止并制止违反国际人道法的行为，并对战争罪进行调查和起诉，包括由平民居民实施的罪行。[80]

[75] Under public international law, a state is responsible for the conduct of private persons, groups, or entities – including civilian hackers or hacker groups – if they are "empowered by the law of that state to exercise elements of the governmental authority", or "in fact acting on the instructions of, or under the direction or control of, that state". See International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, 2001, Articles 5 and 8.

[76] 根据国际公法，一国须对个人、团体或实体（包括平民黑客或黑客团体）的行为负责，前提是他们"经该国法律授权而行使政府权力要素"或"实际上是在按照国家的指示或在其指挥或控制下行事"。见国际法委员会，《国家对国际不法行为的责任条款》，2001 年，第 5 条和第 8 条。

[77] ICRC, Commentary on the Third Geneva Convention, 2020, para. 191 on Article 1.

[78] ICRC, Commentary on the Third Geneva Convention, 2020, para. 183 on Article 1.

[79] 红十字国际委员会，《〈日内瓦第三公约〉评注》，2020 年，关于第 1 条的评注，第 191 段。

[80] 红十字国际委员会，《〈日内瓦第三公约〉评注》，2020 年，关于第 1 条的评注，第 183 段。