国际人道法对网络战的可适用性及其适用

克努特·德尔曼　洛朗·吉塞勒　蒂尔曼·罗登霍伊塞尔*著　丁玉琼**译

摘　要：新技术的快速发展正在改变着我们的社会，也影响着安全及军事格局。在当今的武装冲突中，网络技术的应用已成为现实。网络行动具有特殊的技术特征、可能带来人道代价，特别是针对医疗部门或其他诸如电力、供水或卫生等重要民用基础设施的网络攻击可能会给平民居民造成损害后果。因此，为了保护武装冲突中的平民居民和民用基础设施，承认网络战不是法律空白，而是受到包括国际人道法在内的国际法规范，这一点非常重要。但是，这种新技术的特征给国际人道法规则的解释带来了一些挑战。虽然本文提出了一些解决途径，但是仍然需要进一步的讨论，以澄清既有的国际人道法原则及规则该怎样适用，它们是否恰当且充分，或者是否需要在现有法律的基础上进一步发展。

关键词：网络行动　网络战　国际人道法　可适用性　适用

2019是四项《日内瓦公约》通过70周年。[①]在这70年间，人类社会和生活发生了剧烈的变化，许多变化给国际人道法带来了新的问题和挑战，其中最突出的一个现象是，新技术的快速发展正在改变我们的社会。技术革命，特别是在数字领域的革命，正在深刻地改变我们生活的许多方面，从人际关系到提供服务乃至经济运行方式。一方面，新技术触发了合作及创新，促进了经济发展，也对人道组织的工作产生了积极影响。[②] 例如在中国，移动技术被用于脱贫工作，偏远地区的人们可以在电子商务平台销售他们的农产品。[③] 在中国以及其他国家，线上的高中及大学课程和一些语言课程，也日益让山区儿童有机会获得更高质量的教育。[④] 另一方面，数字化转型也影响着安全及军事格局，在国内和国际层面均是如此。过去几年来，针对私营企业及政府的网

---

*　克努特·德尔曼系红十字国际委员会前首席法律官员、法律部主任；洛朗·吉塞勒系红十字国际委员会高级法律顾问；蒂尔曼·罗登霍伊塞尔系红十字国际委员会法律顾问。本文仅代表作者观点，并不必然代表红十字国际委员会的观点。

**　红十字国际委员会东亚地区代表处高级法律翻译。

① 即《一九四九年八月十二日改善战地武装部队伤者病者境遇之日内瓦公约》（《日内瓦第一公约》）；《一九四九年八月十二日改善海上武装部队伤者病者及遇船难者境遇之日内瓦公约》（《日内瓦第二公约》）；《一九四九年八月十二日关于战俘待遇之日内瓦公约》（《日内瓦第三公约》）；《一九四九年八月十二日关于战时保护平民之日内瓦公约》（《日内瓦第四公约》）。这四项公约一般统称为“日内瓦四公约”。

② See Peter Maurer, “Developing a New Humanitarian Response in the Area of Cyberspace”, 2017, https://www.orfonline.org/wp-content/uploads/2017/11/Our-Common-Digital-Future.pdf (last visited July 2, 2019).

③ 参见“科技扶贫的魔力”，http://www.cpad.gov.cn/art/2017/4/20/art_22_62105.html，最后访问时间：2019年6月17日。

④ 参见“山区小学学生体验在线教育课程”，http://slide.news.sina.com.cn/s/slide_1_2841_88624.html#p=1，最后访问时间：2019年6月17日。

络敌对行动显著增加。这类行动在网络世界及现实世界都产生了影响：它们中断了基础服务，例如电力供应或医疗服务，对某些物体造成实际损害。总体而言，它们给政府和私营部门造成了数十亿美元的损失。

在当今的武装冲突中，网络技术的应用也已成为现实。虽然很多网络行动通常被称为“网络攻击”，但必须强调的是，大多数此类行动与武装冲突毫无关联。但是，某些国家已经公开宣称，有人在当代武装冲突中使用了网络手段，① 而且据说有越来越多的国家正在发展其网络军事能力。② 在冲突中使用网络手段的例子包括：间谍行为；目标识别；影响敌人士气及斗志的信息战；干扰、欺骗或迷惑敌人的通讯系统，以阻碍敌方部队的协同；③ 支援现实作战的网络行动。④ 后者的例子如破坏敌人的军用雷达站以支持空袭行动。⑤

红十字国际委员会首要关注的是构成武装冲突一部分的网络行动。这一关注的焦点来源于红十字国际委员会的使命，其中包括预防武装冲突和其他暴力局势中苦难的发生，并加强国际人道法及普遍人道原则。⑥ 确实，各国一致同意赋予红十字国际委员会的职责要求该组织“为忠实执行适用于武装冲突的国际人道法而努力”，并且“为增进人们对适用于武装冲突之国际人道法知识的了解并促进其传播而努力，并为其发展做好准备”。⑦ 在这一背景下，红十字国际委员会从法律、人道、军事和技术的角度关注新作战手段和方法的发展。关于在武装冲突中使用网络技术，该组织关注以下三个主要问题：（1）鉴于其特殊的技术特征及军事潜力，网络行动可能带

---

① See for example Mike Burgess (Australian signals Directorate), “Offensive cyber and the people who do it”, 27 March 2019, https://www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.htm (last visited July 2, 2019); “Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services”, 14 February 2019, https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf (last visited July 2, 2019); Jeremy Fleming, “Director's Speech at Cyber UK 2018”, 12 April 2018, https://www.gchq.gov.uk/sites/default/files/Director%20CyberUK2018%20As%20Delivered.pdf (last visited July 2, 2019).

② 2015 年《中国的军事战略》白皮书指出，不少国家都在发展网络空间军事力量，中国也将发展防御型网络力量。http://www.gov.cn/zhengce/2015-05/26/content_2868988.htm，最后访问时间：2019 年 6 月 17 日。就一般的评估，见，Anthony Craig, “Understanding the Proliferation of Cyber Capabilities”, Council on Foreign Relations, 2018, https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities (last visited July 2, 2019)。根据联合国裁军问题研究所的报告，2012 年共有 47 个国家组建了网络战部队。United Nations Institute for Disarmament Research, *The Cyber Index*, *International Security Trends and Realities*, UNIDIR/2013/3, Geneva, p. 1.

③ 上海合作组织的成员国多年来一直在关注这些行动。2009 年的《上海合作组织成员国保障国际信息安全政府间合作协定》的第 2 条首次提及“信息武器的研制和使用，信息战的准备与实施”，确定了国际信息安全领域的主要威胁。其附件一将“信息战”定义为“两个或两个以上国家之间在信息空间进行对抗，旨在破坏对方的信息系统、信息运转和信息资源、关键结构和其他结构，动摇对方的政治、经济和社会制度，对其民众进行心理操控，破坏其社会和国家稳定，迫使该国作出有利于敌对方的决定”。参见《上海合作组织成员国保障国际信息安全政府间合作协定》，叶卡捷琳堡，2009 年 6 月 16 日，http://treaty.mfa.gov.cn/Treaty/web/detail1.jsp?objid=1531876097720，最后访问时间：2019 年 6 月 17 日。另见，例如，Jeremy Fleming, “Director's Speech at Cyber UK 2018”。

④ See for example Cox, “US, Coalition Forces Used Cyber Attacks to Hunt Down ISIS Command Posts”, Military.com 25 May 2018.

⑤ Sharon Weinberg, “How Israel Spoofed Syria's Air Defense System”, *Wired*, 4 October 2007; Lewis Page, “Israeli skyhack switched off Syrian radars countrywide”, *The Register*, 22 November 2007.

⑥ 红十字国际委员会的职责与使命是：“红十字国际委员会是一个公正、中立和独立的组织，其特有的人道使命是保护战争和其他暴力事件的受难者，并向他们提供援助。它还致力于通过促进和巩固人道法与普遍人道原则的方式预防苦难的发生。” https://www.icrc.org/en/mandate-and-mission (last visited July 2, 2019).

⑦ 参见《国际红十字会与红新月运动章程》，第 5 条第 3 款和第 7 款。https://www.icrc.org/eng/assets/files/other/statutes-en-a5.pdf (last visited July 2, 2019).

来的人道代价；（2）国际人道法是否可以规范（并且因此限制）网络战；（3）明确国际人道法规则如何限制武装冲突期间网络能力的使用。这就是本文要探讨的三个问题。

一　网络行动可能带来的人道代价

基于网络技术发展迅速的特点及其在武装冲突中可能带来的人道代价，有必要对其进行持续不间断的监测及评估。①

将网络工具作为作战手段或方法为军队提供了这样一种可能性，即不一定需要通过给平民造成直接伤害或给民用设施造成实际损害的方式来达成目标。视具体情况，相较于使用其他作战手段，网络行动更有可能在打击军事目标的同时减少对民用物体的可预见的附带损害。同时，过去几年中发生的网络行动（多数与武装冲突无关）表明，民用设施和基础服务的供给会受到网络攻击的影响。② 这暴露了此类服务的脆弱性。例如，针对医疗部门或工业控制系统的网络行动就有造成人员伤害的风险。

医疗部门看起来尤为脆弱。它们正朝着数字化及互联互通的方向发展，这增加了医疗部门的数字依赖性并扩大了其可能受攻击的范围。很多时候，这些发展与相应的网络安全的提升并不匹配。网络攻击可能对平民居民造成损害的另一个部门是重要的民用基础设施，包括电力、供水和卫生系统。这类基础设施通常是通过工业控制系统来运作的。针对工业控制系统的网络攻击要求特定的专业知识及精细操作，并且通常都是定制的恶意软件。尽管对工业控制系统的攻击不像其他类型的网络行动那样频繁，但据报道其频率正在增加，并且威胁的严重程度比几年前的预期发展得更快。③

在武装冲突中，国际人道法对医疗部门的保护相当全面，并且还禁止攻击民用基础设施，除非该设施已成为军事目标。下文第三（三）部分将详细论述相关的国际人道法规范。

网络所特有的至少三个因素已引起人们的进一步关注：第一，将网络攻击归因于某一国家或非国家行为体已经证明非常具有挑战性（但并非不可能）。④ 这一点不利于识别谁是网络空间中违反了国际人道法的行为者，以及让他们承担法律责任（这是保证遵守国际人道法的一种方式）。合理的借口也会降低使用网络攻击以及违反国际法的门槛。第二，正如中国所指出的，“恶意网络工具和技术扩散的风险与日俱增”。⑤ 网络工具及方法确实可能会以一种很难控制的

① 2018 年 11 月，红十字国际委员会召开专家会议，根据网络技术的特点，对网络能力及其可能的人道后果进行了现实评估。ICRC, Laurent Gisel and Lukasz Olejnik (eds.), *Expert meeting report: The Potential Human Cost of Cyber Operations* (Geneva: ICRC, May 2019), https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf (last visited July 2, 2019).

② 这方面的例子有恶意软件“CrashOverride”“WannaCry”“NotPetya”以及“TRITON”。“CrashOverride”影响了乌克兰的电力供应；“WannaCry”和“NotPetya”影响了好几个国家的医院系统；“TRITON”是旨在干扰工业控制系统的，据报道被用来攻击了沙特阿拉伯的化工厂。有关讨论见，Laurent Gisel and Lukasz Olejnik, ‘The potential human cost of cyber operations: Starting the conversation’, https://blogs.icrc.org/law-and-policy/2018/11/14/potential-human-cost-cyber-operations/ (last visited July 2, 2019)。

③ ICRC, Laurent Gisel and Lukasz Olejnik, *Expert meeting report: The Potential Human Cost of Cyber Operations*, p. 25.

④ 关于归因问题相关国际法规则的讨论，参见下文第三（二）部分。

⑤ 中国代表团孙磊参赞在第 72 届联大一委关于信息和网络安全问题的专题发言，2017 年 10 月 23 日，http://www.china-un.org/eng/chinaandun/disarmament_armscontrol/unga/t1505683.htm (last visited July 2, 2019)。

独特方式扩散。目前复杂的网络攻击只能由最先进、资源最充足的行为者实施。但是，一旦恶意软件被使用、窃取、泄露或者容易获得，除了开发者之外的其他行为者也可能在网上找到该恶意软件，进行反向设计，然后为了自己的目的再利用这些软件。第三，网络行动有过度反应和升级的风险。对于网络攻击的目标来说，我们通常很难确定攻击者的目的是进行间谍活动还是造成其他可能的实际损害。因此存在着这样一种风险，即行动所针对的目标可能会设想最为糟糕的情况，并且作出更为激烈的反应（相较于如果知道攻击者的意图仅仅是间谍活动的情况）。

截至 2019 年年中，网络行动尚未造成重大的人员伤害，但是已经造成了严重的经济损害。[①] 至于网络行动潜在的人道代价，在技术发展方面，由尖端部门（包括军事部门）进行开发的能力和工具方面，以及武装冲突期间使用网络行动的范围可能不同于迄今观察到的趋势方面，我们仍然知之甚少。换句话说，虽然根据目前的观察，人道代价的风险似乎不是很高，但是考虑到冲突总会造成的破坏和痛苦，网络行动的演变既存在不确定性，又变化迅速，因此需要密切关注。

二　武装冲突中国际人道法对网络行动的可适用性

虽然关于国际人道法是否可以适用于网络战（并且因此可以限制网络战）的问题，仍存在争议，[②] 但红十字国际委员会从一开始就采取了明确和肯定的立场。[③] 红十字国际委员会认为，毫无疑问，武装冲突期间的网络行动，或者网络战，都要受到国际人道法的规范，正如冲突中交战方使用的任何武器、作战手段和方法一样，不论新旧。[④] 网络行动依赖于不断发展的新技术这一事实，并不能阻止武装冲突中使用这种技术作为作战手段和方法时国际人道法的适用。

---

① 仅是网络犯罪的总体成本就得以数万亿美元来衡量：据估 2015 年达到了 3 万亿美元，而这个数字在 2021 年将翻倍。Steve Morgan，“Hackerpocalypse：A Cybercrime Revelation”，Herjavec Group，17 August 2016，https：//www. herjavecgroup. com/hackerpocalypse – cybercrime – report/（last visited July 2，2019）．“NotPetya”的影响远远超过 10 亿美元，有人估计高达 100 亿美元 。Fred O'Connor，“NotPetya Still Roils Company's Finances，Costing Organizations billion in revenue”，Cybereason，9 November 2017，https：//www. cybereason. com/blog/notpetya – costs – companies – 1. 2 – billion – in – revenue（last visited July 2，2019）；Andy Greenberg，“The Untold Story of NotPetya，the most devastating cyberattack in history”，“Wired”，22 August 2018，https：//www. wired. com/story/notpetya – cyberattack – ukraine – russia – code – crashed – the – world/（last visited July 2，2019）.

② 红十字国际委员会所理解的“网络战”是指，作为武装冲突背景下的作战手段或方法，通过数据流对计算机系统、网络或其他连接设备所采取的行动。这种理解至少有一部分与《上海合作组织成员国保障国际信息安全政府间合作协定》对信息战的定义是一样的，即信息战是“两个或两个以上国家之间在信息空间进行对抗，旨在破坏对方的信息系统、信息运转和信息资源、关键结构和其他结构”。

③ See ICRC，*International Humanitarian Law and the challenges of contemporary armed conflicts*（Geneva，2011），pp. 36 – 39，https：//www. icrc. org/en/doc/assets/files/red – cross – crescent – movement/31st – international – conference/31 – int – conference – ihl – challenges – report – 11 – 5 – 1 – 2 – en. pdf（last visited July 2，2019）；Knut Dörmann，“Computer network attack and international humanitarian law”，2001，https：//www. icrc. org/en/doc/resources/documents/article/other/5p2alj. htm（last visited July 2，2019）.

④ 国际人道法适用于网络作战手段和方法，如果此种手段和方法构成正在进行的、使用了更为传统的动能手段的武装冲突的一部分的话。单独使用网络行动也可能构成武装冲突并且使国际人道法可以适用。See ICRC，*Commentary on the First Geneva Convention：Convention（I）for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*（Geneva，2nd edn，2016）（hereafter *ICRC Commentary on GC I*），paras. 253 – 256.

在我们看来，国际人道法条约、国际法院的判例以及许多国家和国际组织表达的观点，都给这一结论提供了有力的支持。

国际人道法特有的目的及宗旨就是规范未来的冲突，即那些在国际人道法条约通过之后发生的冲突。当国际人道法条约通过时，缔约国已经纳入了相关的规范，预计可能会出现的新的作战手段和方法并且推定国际人道法可以适用。1868 年的《圣彼得堡宣言》就已经努力将其规定的原则适用于“将来在军备方面的改进”。[①] 在这方面，更为新近且非常重要的一条国际人道法规则是 1977 年《第一附加议定书》第 36 条，[②] 其中规定：“在研究、发展、取得或采用新的武器、作战手段或方法时，缔约一方有义务断定，在某些或所有情况下，该新的武器、作战手段或方法的使用是否为本议定书或适用于该缔约一方的任何其它国际法规则所禁止。”毋庸置疑，这项义务的基础是假设国际人道法适用于这些新的武器、作战手段和方法。否则，就没有必要审查它们在现有法律下的合法性。这其中包括依赖于网络技术的武器、作战手段和方法。

国际人道法适用于网络战这一结论在国际法院所表达的观点中得到了进一步的支持。国际法院在“威胁使用或使用核武器的合法性”咨询意见中认为，适用于武装冲突的既有人道法原则和规则同样适用于“各种形式的战争及各种武器”，包括“未来的武器”。[③] 显然，这其中也包括网络战。

如果国际人道法适用于网络战这一观点被普遍接受，接下来的问题就是是否所有的国际人道法规则都适用还是仅有部分规则适用。在这方面，规范作战手段和方法的国际人道法规则的适用范围大致可以分为：适用于在任何地方均可使用的一切武器、作战手段和方法的规则；以及适用于特定武器（例如各种武器条约）或特定领域（例如海战）的规则。下文将要讨论的规范敌对行动的所有主要的习惯法原则及规则都属于第一类。但是，适用于特定武器或特定领域的国际人道法原则需要更详细的分析。

国际人道法适用于武装冲突中的网络行动，并且因此可以对其进行限制，这一点在国际上得到了越来越多的认可。在 2013 年和 2015 年的联合国《从国际安全角度看信息和电信领域发展政府专家组报告》中，政府专家确认了在网络领域，“国际法，尤其是《联合国宪章》是可以适用的”，并且指出了“既有的国际法律原则，包括可适用的人道原则、必要性原则、比例原则和区分原则”。[④] 越来越多的国家和国际组织已经公开宣称国际人道法适用于网络战。这其中包括欧盟[⑤]和北约。[⑥] 此外，《网络空间信任和安全巴黎倡议》（到 2019 年 5 月已经得到 66 个国家的支持）重申了国际人道法适用于网络战；[⑦] 英联邦政府首脑会议则“承诺会继续讨论可适用的国际

① 《关于在战争中放弃使用某些爆炸性弹丸的宣言》，圣彼得堡，1868 年 11 月 29 日—12 月 11 日。

② 《1949 年 8 月 12 日日内瓦四公约关于保护国际性武装冲突受难者的附加议定书》（第一议定书），1977 年 6 月 8 日。

③ International Court of Justice, *Legality of the threat or the use of nuclear weapons*, Advisory Opinion, 8 July 1996, para. 86.

④ Note by the Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (2013), para. 19; A/70/174 (2015), para. 28.

⑤ EU Council Conclusions, General Affairs Council meeting, 25 June 2013, 11357/13.

⑥ NATO, *Wales Summit Declaration* (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014, para. 72, https://www.nato.int/cps/en/natohq/official_texts_112964.htm (last visited July 2, 2019).

⑦ https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (last visited July 2, 2019).

人道法如何适用于网络空间的各个方面”。[①] 虽然俄罗斯国防部于 2011 年表示，在全球信息空间的军事活动中，“俄罗斯联邦的武装部队会遵守国际人道法”，[②] 但是到目前为止，俄罗斯尚未作出确定的法律声明。[③]

中国在亚非法律协商组织（以下简称亚非法协）的声明给人的印象是，中国在这个问题上还没有一个完全确定的立场。在 2015 年的亚非法协第 54 届年会期间，在“网络空间的国际法问题”的特别会议上，中国提出：“关于网络空间中的使用武力问题，现行法，包括国家诉诸战争权和战时法，原则上都适用于网络空间。同时，对于网络这一‘蛮荒之地’，有必要制定新的规则”。[④] 一年以后，在亚非法协第 55 届年会的网络空间国际法问题开放式工作组的会议上，中国表示：“关于网络战，目前缺乏国际共识及国家实践，所以中国并不赞同将自卫权和武装冲突法适用于网络空间。”[⑤] 最近，在红十字国际委员会和中国社会科学院国际法研究所共同举办的“纪念日内瓦四公约 1977 年《附加议定书》通过 40 周年国际研讨会”上，一位中国官员以个人观点表示：“国际人道法规则的适用范围扩大，已经扩大到网络空间。联合国信息安全专家组在其 2013 年和 2015 年的报告中均确认，国际法特别是《联合国宪章》适用于网络空间。因此，国际人道法原则上应适用于网络攻击，但如何适用还值得探讨。”[⑥]

在这种讨论的背景下，许多国家包括中国在内，都明确表示反对网络空间的军事化，或者网络军备竞赛，而且关注避免将网络军事行动合法化。[⑦] 但是，在我们看来，断言国际人道法适用于网络战并不是鼓励网络空间军事化，并且不得以任何方式将其理解成网络战合法化。国家诉诸任何武力都要受到《联合国宪章》的规范，不论发生在网络空间还是现实世界。除了（以及独立于）《联合国宪章》的要求之外，如果国家和/或非国家武装团体在武装冲突期间采取网络行动，国际人道法就可以对敌对行动有所限制。特别是，国际人道法通过限制交战各方对作战手段和方法的选择，来保护平民及民用物体免遭敌对行动的影响，不论使用武力是否合法。这意味着，与将武装冲突中的网络行动（或者任何其他军事行动）合法化恰恰相反，除了《联合国宪

---

① Commonwealth Heads of Government Meeting, *Commonwealth Cyber Declaration*, London, 20 April 2018, p. 4, para. 4, http://thecommonwealth.org/commonwealth-cyber-declaration (last visited July 2, 2019).

② Ministry of Defense of the Russian Federation, *Russian Federation Armed Forces' Information Space Activities Concept*, 2011, section 2.1. 另外，俄罗斯于 2011 年提出了《国际信息安全公约》（概念）草案，其中第 7 条第 2 款规定，在任何国际冲突中，卷入冲突的缔约国都有权选择受可适用的国际人道法规范约束的“信息战”手段。www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (last visited July 2, 2019).

③ 参见俄罗斯代表弗拉基米尔·叶尔马科夫在第 72 届联大一委上关于“其他裁军措施及国际安全”的发言（没有官方翻译），2017 年 10 月 3 日；“负责信息安全国际合作的俄罗斯总统特别代表安德烈·克鲁茨基克对塔斯社关于此领域国家间对话问题的回应”，2017 年，http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288 (last visited July 2, 2019).

④ AALCO/54/BEIJING/2015/VR, Verbatim Record of Discussions, p. 177.

⑤ AALCO/55/NEW DELHI (HEADQUARTERS) /2016/VRf, Verbatim Record of Discussions, p. 159.

⑥ 马新民：《变革中的国际人道法：发展与新议程——纪念〈日内瓦公约〉1977 年〈附加议定书〉通过 40 周年》，载《国际法研究》2017 年第 4 期，第 8 页。

⑦ See, for example, *Position Paper of the People's Republic of China For the 73rd Session of the United Nations General Assembly*, p. 10, http://www.chinesemission-vienna.at/eng/zgbd/P020180830583238976576.pdf (last visited July 2, 2019); Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 23, 2017, p. 2; 俄罗斯联邦外交部，“负责信息安全国际合作的俄罗斯总统特别代表安德烈·克鲁茨基克对塔斯社关于此领域国家间对话问题的回应”。

章》和习惯法（诉诸战争权）之外，国际人道法（战时法）另外规定了限制。

国际人道法可以适用的事实并不妨碍各国进一步发展完善国际人道法，或就自愿规范达成协议，或者致力于对现有规则共同作出解释。例如，在2018年关于信息和通信技术应用安全的开放式工作组设立时，联合国大会就表示“欢迎”联合国政府专家组历经数年所制定的一套“国家负责任行为的国际规则、规范和原则”（共有13项）。[①] 信息安全领域可能产生新规则的另一个例子，是中国、俄罗斯联邦、塔吉克斯坦和乌兹别克斯坦于2011年向联合国提交的《信息安全国际行为准则》。根据该准则，各国将承诺“不扩散信息武器及相关技术”。[②]

具体到国际人道法，确定现有的原则和规则如何适用这个问题需要更深入的讨论：它们是否恰当且充分，或者是否需要在现有法律的基础上进一步发展。

三　国际人道法对武装冲突中使用网络能力的限制

承认国际人道法原则上适用于与武装冲突有联系的网络行动只是第一步。这一新技术的具体特点给国际人道法规则（包括敌对行动规则）的解释带来了若干挑战，需要具体讨论。

（一）国际人道法规范哪些网络行动

国际人道法只适用于构成武装冲突一部分的网络行动，或者说构成武装冲突的网络行动（目前这还不太可能）。

在已有的、通过现实手段进行的国际性或非国际性武装冲突背景下（并且与之相关联）开展网络行动时，相关的国际人道法规则可以规范该行动。[③]

另一个单独的问题是当这些行动与正在进行的武装冲突无关时，国际人道法是否可以规范单独的网络行动（没有现实的行动）。这个问题需要在规范国际性和非国际性武装冲突的1949年日内瓦四公约共同第2条和第3条的基础上，分别分析。[④] 这两种类型的武装冲突在参与方的性质、导致国际人道法适用于这类冲突的暴力的激烈程度和可适用的国际人道法规则方面，都有所不同。

关于国际性武装冲突，红十字国际委员会认为，我们没有任何理由区别对待导致民用或军事资产损毁，或者士兵或平民死亡或受伤的一起或多起网络行动，与通过更传统的作战手段和方法

① 联合国大会决议：《从国际安全角度看信息和电信领域的发展》，A/RES/73/266（2018）。

② http：//nz. chineseembassy. org/eng/zgyw/t858978. htm（last visited July 2，2019）. 2013年哈萨克斯坦和吉尔吉斯斯坦加入成为共同提案国。另一明确提及国际人道法的提案，参见俄罗斯2011年提出的《国际信息安全公约》（概念）第7条。更一般而言，参见联合国《从国际安全角度看信息和电信领域发展政府专家组报告》以及第73届联合国大会上通过的两个决议：《从国际安全角度促进网络空间国家负责任行为》，A/RES/73/27（2018）；《从国际安全角度看信息和电信领域的发展》，A/RES/73/266（2018）。

③ See *ICRC Commentary on GC I*，para. 254；Michael N. Schmitt and Liis Vihul（eds.），*Tallinn Manual 2. 0 on International law applicable to cyber operations*（Cambridge：Cambridge University Press，2nd edn，2017）（hereafter *Tallinn Manual 2. 0*），Rule 82. 红十字国际委员会欢迎各位专家重申国际人道法与网络战的相关性，并且表示希望《塔林手册》能有助于各国就这些具有挑战性的问题做进一步讨论。

④ 日内瓦四公约共同第2条第1款规定：“本公约适用于两个或两个以上缔约国间所产生之一切经过宣战的战争或任何其他武装冲突，即使其中一国不承认有战争状态”；共同第3条第1款规定：“在一缔约国之领土内发生非国际性的武装冲突之场合……”。

所进行的同等攻击。[①] 但是，在单独的网络行动（与正在进行的包含现实行动的武装冲突无关，并且不会产生与现实行动相类似的影响——例如只会干扰但不会毁坏民用或军事设施的网络行动）是否受到适用于国际性武装冲突的国际人道法的规范（并因此受限制）这个问题上，国家实践仍不明朗。[②]

至于非国际性武装冲突，则产生了各种各样的问题。第一，非国际性武装冲突可能仅存在于充分有组织性的各方之间。虽然国家武装部队满足有组织性的要求，但是非国家武装团体则需要仔细加以研究。当武装团体只是在网上组织时，要确定有组织性就变得非常具有挑战性（但并非不可能）。[③] 第二，适用于国际性武装冲突的国际人道法规范国家间任何诉诸武力的行为但不考虑其激烈程度，[④] 与此不同，只有两个或多个有组织的参与方之间的暴力达到足够的激烈程度，非国际性武装冲突才会存在。此外，尽管在例外情况下也有可能，但要是说仅有网络行动就能满足非国际性武装冲突的激烈程度要求，仍然不太现实。[⑤]

（二）归因问题

一般而言在战争中（特别在网络战中），国家有时会利用非国家行为体（例如非国家武装团体或私营军事安保公司）来开展某些行动，包括网络行动。网络空间的特殊性质，例如行为者隐藏或伪造其身份的各种可能性，使得将行为归因于特定个人或武装冲突各方的问题变得极为复杂。[⑥] 在确定某一局势中国际人道法的可适用性时，这个问题带来了巨大的挑战。如果不能确定特定行动的行为者（从而不能确定该行动与武装冲突之间的联系），那么就极难确定国际人道法是否适用于该行动。第一，将一个国家或非国家的网络攻击定性为武装冲突要适用不同的暴力程度门槛。因此，除非知道某一行动的国家或非国家的性质，否则就不清楚该适用哪一门槛。此外，适用于国际性与非国际性武装冲突的某些国际人道法规则是不一样的。第二，即使发生了武装冲突，与该冲突没有关联的网络攻击（例如与冲突无关的犯罪行为）是不受国际人道法规范的。无法确定网络行动的行为者可能会妨碍确认与冲突的联系是否存在。这些示例表明，确定谁是网络行动的行为者，以及该行动是否可以归因于冲突的国家或非国家一方，具有重要的法律意义。

国际人道法并没有定义具体的标准来确定个人或非国家行为体是否代表国家行事。因此，必须要在规范归因问题的一般国际法规则中寻找答案，其中最为细化的是国家责任法。根据习惯国际人道法和一般国际法，国家需要为以下违反国际人道法且可归因于它的行为负责，

---

① *ICRC Commentary on GC I*, para. 255; *Tallinn Manual 2.0*, Rule 83, para. 15.

② 正如前文所述，与正在进行的武装冲突无关的网络行动的合法性必须依据《联合国宪章》及其他法律体系而不是国际人道法来分析。

③ *ICRC Commentary GC I*, para. 437. 对这个问题更进一步的分析见，Tilman Rodenhäuser, *Organizing Rebellion* (Oxford: Oxford University Press, 2018), pp. 104 – 108。

④ *ICRC Commentary on GC I*, paras. 236 – 244.

⑤ *ICRC Commentary on GC I*, para. 437. 进一步的讨论见，Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians", (2012) 94 *International Review of the Red Cross* 533, p. 551. Michael N. Schmitt, "Classification of Cyber Conflict", (2012) 17 *Journal of Conflict and Security Law* 245, p. 260。

⑥ 关于将网络攻击归于特定行为者的技术挑战的审查，见，Vitaly Kamluk, "Know your enemy and know yourself: Attribution in the cyber domain", https://blogs.icrc.org/law – and – policy/2019/06/03/know – your – enemy – know – yourself – cyber – domain – attribution/ (last visited July 2, 2019)。

包括：（1）国家机关的行为，包括武装部队；（2）行使政府权力要素的个人或实体的行为；（3）事实上受到国家指示，或者在国家指挥或控制下的个人或团体的行为；以及（4）国家承认和当作其本身行为的私人或团体的行为。[①] 不论违反国际人道法的行为是通过网络手段还是任何其他手段实施的，这个结论都成立。

（三）规范敌对行动的国际人道法规则的可适用性及“攻击”的概念

由于缺乏专门规范网络行动的国际人道法规则，在解释国际人道法一般规则并将其适用于此类行动时，存在着很多挑战。

虽然很多关于敌对行动的一般规则仅限于国际人道法所界定的构成攻击的行为，但是有些规范敌对行动的国际人道法规则适用于所有的军事行动，大多数是那些对某类物体提供特别保护的规则。

这类规则的一个例子，是国际人道法关于保护居民赖以生存的医疗服务或物体的具体规定。对大多数军事行动而言，这些规定提供了相当广泛的保护，包括并不构成攻击的行动。鉴于医疗服务对受武装冲突影响的平民至关重要，交战各方在任何时候都必须尊重及保护医疗设施和医务人员。[②] 在武装冲突中，大多数情况下针对医疗部门的网络攻击都是违反国际人道法的。同样，除了禁止攻击任何民用物体的一般性规定之外，国际人道法规则还专门规定，禁止攻击、毁坏、移动对平民居民生存所不可缺少的物体或使其失去效用。[③]

但是，一项行动是否构成“攻击”这个问题，对于源自为平民和民用物体提供重要保护的区分原则、比例原则和预防措施原则的很多规则的可适用性来说，至关重要。具体来说，在进行攻击时，禁止攻击平民和民用物体，[④] 禁止不分皂白[⑤]及不成比例的攻击，[⑥] 以及采取一切可能的预防措施以避免或尽量减少平民受伤害和民用物体受损害的义务，适用于所有那些构成国际人道法所定义之“攻击”的行动。因此，就网络行动而言，“攻击”的概念是广义解释还是狭义解释的问题，对于重要规则对各种网络行动的可适用性以及这些规则对平民或民用设施提供的保护来说，十分重要。但迄今为止，很少有国家对国际人道法中攻击的概念该如何适用于网络行动阐明详细观点。[⑦]

---

① 参见让－马里·亨克茨与路易丝·多斯瓦尔德－贝克：《习惯国际人道法第一卷——规则》（以下简称《习惯国际人道法研究》），法律出版社 2007 年版，规则 149。另见国际法委员会：《国家对国际不法行为的责任》，2011 年，特别是第 4 条至第 11 条。

② 参见，例如《日内瓦第一公约》第 19 条；《日内瓦第二公约》第 12 条；《日内瓦第四公约》第 18 条；《第一附加议定书》第 12 条；《1949 年 8 月 12 日日内瓦四公约关于保护非国际性武装冲突受难者的附加议定书》（《第二附加议定书》，1977 年 6 月 8 日）第 11 条；《习惯国际人道法研究》规则 25、28 和 29。

③ 参见《第一附加议定书》第 54 条；《第二附加议定书》第 14 条；《习惯国际人道法研究》规则 54。

④ 参见《第一附加议定书》第 52 条；《习惯国际人道法研究》规则 7—10。

⑤ 参见《第一附加议定书》第 54 条第 3 款；《习惯国际人道法研究》规则 11。

⑥ 参见《第一附加议定书》第 51 条第 5 款第 2 项；《习惯国际人道法研究》规则 14。

⑦ 澳大利亚认为规范攻击的国际人道法规则可适用于网络行动，“只要该行动达到了国际人道法中现实‘攻击’（或暴力行为）同样的门槛”。Commonwealth of Australia, Department of Foreign Affairs and Trade, “Australia's International Cyber Engagement Strategy”, 2019, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_international_law_supplement.html (last visited July 2, 2019). 2015 年版的美国国防部《战争法手册》认为，可以破坏敌方电脑系统的网络攻击是国际人道法中的“攻击”，而丑化政府网页，轻微、短暂地中断互联网服务，短暂中断、禁用或干扰通信，以及进行宣传等行为不是攻击，并且因此可以直接针对平民或民用物体。U.S. Department of Defense, *Law of War Manual* (2015, updated December 2016), paras. 16.5.1 and 16.5.2.

《第一附加议定书》第 49 条将攻击定义为“不论在进攻或防御中对敌人的暴力行为”。目前可以确定的是，这个定义中的“暴力”概念既可以指作战手段，也可指其效果，这意味着产生暴力效果的行动就可以构成攻击，即使导致该效果的手段并不是在现实世界采取的。①

有人主张，所有预期造成死亡、伤害或实际损害的行动都构成攻击，包括此种损害是由于攻击可预见的间接效果所造成的情况，例如针对电网的网络攻击切断了医院的电力供应而造成重症监护病房病人的死亡。但是，对于会导致功能丧失却并没有造成实际损害的网络行动是否构成国际人道法中所定义的攻击这个问题，则仍有争论。②

红十字国际委员会认为，在武装冲突中，旨在使电脑或电脑网络功能失效的行动构成有关敌对行动的国际人道法规则意义上的攻击，不论该物体是因为现实手段还是网络手段而失能的。③该解释基于以下两个主要理由。

第一个理由源自根据上下文对攻击这一概念的解释。④ 考虑到《第一附加议定书》第 52 条第 2 款中定义的“军事目标”不仅将毁坏或缴获，而且将“失去效用”作为攻击的可能结果，《第一附加议定书》第 49 条中的“攻击”概念也应当被理解为包含旨在损害物体功能（也就是使其失去效用）但未造成物理损害或毁坏的行动。否则，《第一附加议定书》第 52 条第 2 款明确提及失去效用就多余了。因此，某一物体是因为毁坏还是其他方式而失去效用，这一点无关紧要。⑤

第二个理由是，过于严格地理解攻击的概念很难与敌对行动规则的目的及宗旨保持一致，而这些规则旨在确保平民居民和民用物体免受敌对行动的影响。的确，根据这种过于严格的理解，旨在使民用网络（电力、银行、通讯或其他网络）失去效用或有附带造成这种结果之风险的网络行动，可能不属于保护平民居民及民用物体的国际人道法基本规则的范畴。⑥

同时，不是所有武装冲突中的网络行动都会构成国际人道法意义上的“攻击”。国际人道法中的攻击概念并不包括间谍行为。此外，敌对行为规则没有禁止干扰民用通讯系统的所有行动：干扰无线电通讯或电视广播在传统意义上并不会被认为是国际人道法所定义的攻击。

（四）保护“民用物体”免遭网络攻击：区分原则、攻击“军民两用”物体以及将数据视作“物体”

区分原则作为国际人道法的基本原则，规定“冲突各方无论何时均应在平民居民和战斗员

---

① Cordula Droege，“Get off my cloud”，p. 557；William Boothby，*The Law of Targeting*（Oxford：Oxford University Press，2012），p. 384.

② See *Tallinn Manual 2. 0*，commentary on rule 92，paras 10 – 12.

③ See ICRC，*International humanitarian law and the challenges of contemporary armed conflicts*（Geneva，2015）（hereafer *ICRC IHL Challenges Report 2015*），pp. 41 – 42，https：//www. icrc. org/en/download/file/15061/32ic – report – on – ihl – and – challenges – of – armed – conflicts. pdf（last visited July 2，2019）.

④ 《维也纳条约法公约》第 31 条第 1 款。

⑤ See also，Knut Dörmann，“Applicability of the Additional Protocols to Computer Network”，2014，p. 4，https：//www. icrc. org/en/doc/assets/files/other/applicabilityofihltocna. pdf（last visited July 2，2019）；Cordula Droege，“Get off my cloud”，p. 559. 一种不同的观点见，Michael N. Schmitt，“Cyber Operations and the *Jus in Bello*：Key Issues”，（2011）87 *Naval War College International Law Studies* 89，pp. 95 – 96。

⑥ See also Michael N. Schmitt，“Wired warfare 3. 0：Protecting the civilian population during cyber operations”，（2019）*International Review of the Red Cross* 1，p. 7，doi：10. 1017/S1816383119000018.

之间和在民用物体和军事目标之间加以区别，因此，冲突一方的军事行动仅应以军事目标为对象。”[①]《第一附加议定书》第 52 条第 1 款重申“民用物体不应成为攻击或报复的对象”，并且将“民用物体”定义为“所有不是军事目标的物体”。如前文所述，虽然越来越多的人承认区分原则以及其他国际人道法基本原则适用于网络战，但是网络空间某种程度上的非物理（数字）性质以及该空间中军事及民用网络的相互关联性，使得在适用及解释这些规则时产生了很多实践及法律上的挑战。

在网络战的背景下，时有争论认为，网络空间的互联互通性使得实施区分民用物体及军事目标的国际人道法基本规则以及避免给平民带来过分附带损害的义务变得极具挑战性（但并非不可能）。正如下文将讨论的，这种挑战可能被夸大了（下文第 1 点）。尽管如此，就保护重要的民用网络基础设施免受军事攻击而言，仍然有两个关键的问题。第一，对于数据是否构成国际人道法意义上的“物体”，尚存在分歧（下文第 2 点）；第二，关于敌对行为的国际人道法规则如何适用于同时具有民用和军事目的的物体（通常被称为军民两用物体，这在网络空间中尤为普遍），对这个问题一直存在争论（下文第 3 点）。

1. 从技术角度看，网络攻击可以针对特定的军事目标

实施区分原则、比例原则以及禁止不分皂白攻击的规则，要求该攻击可以针对且实际针对军事目标，而且不会给平民或民用物体造成过分的附带损害。与这些原则可能在网络空间中没有意义（由于网络空间的互联互通性）的推断正相反，[②] 对网络工具之功能的审慎检查表明，它们并非天然就不分皂白。

恶意软件的开发者或网络攻击的计划者可以将工具设计成不带自我传播功能的。这样的话，如果没有额外的人工干预，恶意软件就无法传播。过去几年的攻击显示，恶意软件可以被设计成仅攻击特定的硬件或软件。这意味着，即使恶意软件被编程为可以广泛传播的，它们仍然可以被设计成只对特定的目标或目标集造成损害。特别是旨在对工业控制系统造成损害的网络攻击，可能需要为特定目标和目的而设计的网络工具。在许多情况下，从技术的角度来看，对这种定制工具的需求将有效地遏制大规模或不分皂白地实施攻击的能力。网络攻击在技术上可以实现精确打击这一事实并不意味着，如果在冲突中实施这种攻击，就必然合法。但是，我们在很多网络行动中所观察到的特点表明，它们很可能是特别精确定制的，只对特定的目标产生影响，并且因此有能力符合国际人道法的原则和规则的要求。

有些已知的网络工具被设计成可以自我传播，并且可以对广泛使用的民用电脑系统造成损害后果。但是，这些恶意软件并不支持这一论点，即网络空间的互联互通性使得国际人道法基本规则的实施变得很有挑战性，如果不是不可能的话。相反，在武装冲突中，使用这种网络工具可能是国际人道法所禁止的。[③] 的确，国际人道法禁止不能针对具体军事目标或者可能预计脱离使用

① 《第一附加议定书》第 48 条；《习惯国际人道法研究》规则 7。

② See, for example, Robin Geiss and Henning Lahmann, “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space”, (2012) 45 *Israel Law Review* 381.

③ 相类似的，美国国防部《战争法手册》规定，例如，一种破坏性的计算机病毒被编程为在民用互联网系统内不受控制地传播和摧毁，则将被作为不分皂白的武器而受禁止。U. S. Department of Defense, *Law of War Manual*, para. 16. 6.

者控制的,[①] 或者当攻击军事目标时预计造成与预期的具体和直接军事利益相比过分的附带平民损害的作战手段和方法，包括网络手段和方法。[②]

2. 将数据作为“民用物体”加以保护

数据是数字领域的重要组成部分，而且是很多社会生活的基石：个人医疗数据、社会保障数据、纳税记录、银行账户、公司客户档案或候选人名单及记录，这些是公民生活有效运转的关键。人们越来越关注保护这些基本的民用数据。

就属于受到国际人道法特别保护的某类物体的数据而言，保护的规则是很全面的。例如，尊重和保护医疗设施的义务必须被理解为延伸到属于这些设施的医疗数据。[③] 与此类似，禁止删除或篡改数据以致使对于平民居民生存来说不可缺少的物体如饮用水装置、供水设施和灌溉工程失去效用。[④]

但是澄清下面这个问题很重要：即没有从这种具体保护中获益的民用数据在多大程度上受到关于敌对行为的既有的一般规则的保护。特别是，围绕着数据是否构成物体，以及针对数据的网络行动（例如删除数据）是否受到区分原则、比例原则及预防措施原则及其为民用物体所提供的保护所规范等问题，目前存在广泛的争论。[⑤]

删除或篡改这种数据可能会迅速使政府服务及私营企业陷入彻底停顿，而且相比实际物体的损毁，可能会给平民造成更多的损害。在今天这个越来越依赖网络的世界里，国际人道法并不禁止这种行动的结论——不论是因为删除或篡改这些数据并不构成国际人道法意义上的“攻击”，还是因为这些数据并不会被视作禁止攻击民用物体意义上的“物体”，看起来都很难符合这一法律制度的目的及宗旨。[⑥] 用数字数据替换纸质文件和文档不应减少国际人道法为它们所提供的保护。[⑦]

3. 对同时用于军事及民用目的的网络设施的保护

为了保护依赖于网络空间的重要民用基础设施，保护网络基础设施本身也是非常重要的。但是，这个问题的挑战在于民用和军用网络的互联互通性。大多数军用网络依赖于民用网络设施，例如海底光纤电缆、卫星、路由器或节点。民用车辆、船舶和空中交通管制的导航系统越来越依赖于全球导航卫星系统，例如北斗、格洛纳斯系统（俄国版的全球导航卫星系统）、全球定位系统或伽利略导航卫星系统，这些系统也可能被军方使用。民用物流供应链（食品和医疗供给）及其他企业也会与一些军事通信共用相同的网络和通信网络。除了特别用于军事用途的某些网络之外，在很大程度上，要想区分纯民用和纯军用网络基础设施是不可能的。

---

① Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva and Dordrecht: ICRC/Martinus Nijhoff Publishers, 1987) (hereinafter *Commentary on the Additional Protocols*), para. 1963.

② 《第一附加议定书》第 51 条第 4 款及第 5 款；《习惯国际人道法研究》规则 11 和规则 14。

③ 参见，例如《日内瓦第一公约》第 19 条；《第一附加议定书》第 12 条；《习惯国际人道法研究》规则 28。

④ 《第一附加议定书》第 54 条；《第二附加议定书》第 14 条；《习惯国际人道法研究》规则 54。

⑤ See *Tallinn Manual 2.0*, commentary on Rule 100, paras. 6 – 7. 有关学术讨论见，(2015) 48 *Israel Law Review* 39, pp. 39 – 132; Michael N. Schmitt, “Wired warfare 3.0: Protecting the civilian population during cyber operations”.

⑥ *ICRC IHL Challenges Report 2015*, p. 43.

⑦ 例如，法国提出，某些数据内容虽然是无形的，但仍可被视为国际人道法下受保护的民用物体。https://www.diplomatie.gouv.fr/IMG/pdf/190514 – _ french_ reponse_ un_ resolutions_ 73 – 27_ – _ 73 – 266_ ang_ cle4f5b5a – 1.pdf (last visited July 2, 2019).

根据国际人道法，攻击必须严格限于军事目标。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。根据国际人道法，只要不符合该定义的所有物体都是民用物体，并且不应成为攻击或报复的对象。对通常用于民用目的的物体，在其是否对军事行动作出有效贡献的问题存在怀疑时，该物体应推定为民用物体并因此受到保护。①

传统的理解是，某一物体如果用作军事目的而满足军事目标的定义，那么该物体就构成军事目标，即使其同时也用于民用目的。对这一规则的广义解释可能会得出这样的结论：构成网络基础设施一部分的许多物体都可能成为军事目标，并且因此不再享有免遭攻击的保护，不论是网络攻击还是现实攻击。因为平民对网络空间的依赖日益增加，这将会是人们严重关切的一个问题。

但是，这个结论是不完整的。第一，这一分析不能针对网络空间或整个互联网而进行，但是交战各方必须确定哪些具体的计算机、节点、路由器或网络可能成为军事目标。在这方面，需要单独分析可从网络或系统中分离出来的网络的部件、特定计算机或其他硬件。第二，网络的设计具有高度冗余性，意味着其特点之一就是数据流迅速改道的能力。按照军事目标定义的要求，在评估目标的损坏或失去效用是否会实际提供明确的军事利益时，需要考虑这种内置的恢复能力。如果不是这样，该物体仍然是民用物体，不能受到攻击。第三，任何攻击都应受到禁止不分皂白攻击的规则以及攻击中的比例原则及预防措施原则的规范。即使某一物体已经成为军事目标，违反这些原则之一从而终止或损害民用物体的利用，都构成非法的攻击。②

（五）为确保尊重国际人道法而对网络作战手段和方法进行法律审查的重要性

鉴于网络空间的特点给某些关于敌对行为的国际人道法原则的解释及适用所带来的特别挑战，武装冲突的各方在开发及使用网络工具作为作战手段和方法的过程中需要仔细审查。在这方面，正如前文所提到的，发展或获取网络作战能力的《第一附加议定书》的缔约国（不论是出于进攻还是防御的目的）都有义务评估网络武器、作战手段与方法的部署是否在某些或一切情形下为国际法所禁止。③ 更宽泛而言，对于国家来说，进行法律审查以保证尊重国际人道法是至关重要的，这意味着武装部队仅能根据该国承担的国际人道法义务开发和使用网络作战手段或方法。这种审查应当囊括多学科团队，包括相关的法律、军事及技术专家。为了分析具体实施攻击时实际使用的工具的合法性，就需要进行这些法律审查，而且审查要更为深入细致。

---

① 参见《第一附加议定书》第52条；《习惯国际人道法研究》规则7—10。

② ICRC, Laurent Gisel (ed.), *International Expert Meeting Report*, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law* (Geneva: ICRC, 2018), p. 39, https://www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality (last visited July 2, 2019); See also Helen Durham, "Keynote address", in Edoardo Greppi (ed.), *Conduct of Hostilities: The Practice, the Law and the Future* (Franco Angeli: International Institute of Humanitarian Law, 2015), p. 31.

③ 《第一附加议定书》第36条。

网络武器、作战手段和方法的法律审查可能面临着许多挑战。以下我们列举了一些挑战，但没有穷尽：

第一，进行法律审查的国家需要确定采用什么样的法律标准来审查某一网络工具。换句话说，对于前文讨论的一些问题，缔约国需要有答案，例如使用网络工具是否构成攻击并且因此需要遵守某些特定的国际人道法规则。

第二，对一种武器的评估不应脱离其使用的方式，这意味着在法律审查中必须要考虑武器正常及预期的使用方式。但是，相较于动能武器，网络军事能力可能没有那么标准化，尤其是设计用于某一特定行动的情况。这意味着需要根据其可能使用的特定网络环境而进行审查。

第三，与此相关的是，缔约国不仅应当对其将要首次使用的武器进行法律审查，而且应当包括已经通过法律审查但有所改动的武器。相关的网络工具可能会频繁地调整，这可能会给国家带来挑战，包括应对潜在目标将进行的软件安全升级。虽然可能需要进一步明确类型及范围变化而需要新的法律审查这一问题，但是已经有人指出，“对一种变化是否会影响程序运行的评估必须是定性的，而不是定量的”。①

为了使法律审查有效，发展或使用新武器技术的国家需要处理这些问题以及其他复杂的问题。换句话说，测试制度必须适应网络技术的独特性。鉴于上述复杂性，保证所有国家尊重国际人道法的最佳实践就是共享一国法律审查机制的相关信息，并且在可行范围内，共享法律审查的实质性成果。在出现武器与国际人道法不相符的问题时，这一点尤其重要，从而避免其他国家遇到同样的问题，以及将试验国关于国际人道法禁止此类工具的结论通知其他国家。

四　结论

为了保护武装冲突中的平民居民和民用基础设施，承认网络战不是法律空白，而是受到包括国际人道法在内的国际法规范，这一点非常重要。但是，正如本文所论，承认国际人道法的可适用性并不是讨论的终结。关于国际人道法在网络空间中如何解释，我们需要更多的讨论（特别是国家间的讨论）。任何这种讨论都应依据对网络军事能力的发展、它们可能造成的人道代价以及既有法律已经提供的保护的深入了解。红十字国际委员会认为，承认国际人道法适用于网络空间，讨论如何解决网络空间的具体特征所带来的各种挑战以及既有法律是否恰当充分，并不排除新的规则可能是有用甚至是必要的。但是，如果制定新的规则，这应当建立在既有法律框架之上，并且能够加强既有法律框架（包括国际人道法）。当然，红十字国际委员会已准备好为此类讨论提供一些专业知识。

① Gary D. Brown and Andrew O. Metcalf, “Easier said than done: legal reviews of cyber weapons”, (2014) 7 *Journal of National Security Law and Policy* 115, p. 133.

Applicability and Application of International Humanitarian Law to Cyber Warfare

Knut Dörmann, Laurent Gisel and Tilman Rodenhäuser, translated by Ding Yuqiong

Abstract: The ever-faster development of new technologies is transforming societies. It is also affecting the security and military landscape, and the use of cyber technology has become a reality in today's armed conflicts. This article explores first the specific technical characteristic of cyber operations and their potential human cost. In particular, cyber attacks against the healthcare sector or other critical civilian infrastructure such as electricity, water or sanitation can have harmful effects on the civilian population. For the protection of the civilian population and civilian infrastructure during armed conflicts, it is therefore critical to recognize that cyber warfare do not occur in a legal void but is regulated by international law, including international humanitarian law (IHL). The specific characteristics of this new technology however raise several challenges for the interpretation of IHL rules. While the article proposes some avenues, further discussions may be needed to clarify how existing IHL principles and rules apply, whether they are adequate and sufficient, or whether further development the law is needed.

Keywords: Cyber Operations, Cyber Warfare, International Humanitarian Law, Applicability, Application

(责任编辑：孙世彦)