INTERNATIONAL REVIEW of the Red Cross

区分原则在网络背景中的适用：一个中国视角

黄志雄、应瑶慧*著/应瑶慧**译

摘要

截至目前，中国政府对国际人道法在网络空间的适用问题只做了一般性的评价。确有一些中国学术论文涉及此话题，但对区分原则的讨论在篇幅和学术深度上都较为有限。与西方相比，中国学者对此话题的研究尚处于比较初级的阶段。目前，中国学术界还没有对区分原则在网络空间中的适用进行具体的解构或澄清。作为首篇由中国学者撰写的专门研究该问题的论文，此文通过注入中国官方立场和中国学者观点，提供了一个不同的视角。作者的目的是澄清现有规则是否仍然完全适用于网络背景，如果需要，找出可以做出什么样的改进和澄清。在权衡这些争论时，我们认为，尽管存在潜在的技术挑战和不确定性，但区分原则应适用于网络空间。还应从防止过度军事化和最大限度地保护平民利益的立场上仔细重新审查和澄清。对于人类目标，习惯国际法和相关条约中确定战斗员身份的要素并不非常适合数字战场。然而，网络战斗员仍然有义务将自己与平民区分开来。在适用区分原则时，我们认为将重点放在实质性因素上比放在形式因素上更有意义，例如公开携带武器或备有可从远处识别之固定的特殊标志。在解释“直接参加敌对行动”时，损害门槛要求有客观可能性，而不只是主观意图；交战联系应该被确认，因果关系应该是近因。类比适用“网络杀伤链”模型，有助于我们把握网络战中直接参加敌对行动的全过程。对于非人类目标，所有军事目标都必须同时满足“实际贡献”和“明确的军事利益”标准，这两者同样不可或缺。同样的要求也适用于军民两用物体。此外，某些数据应属于民用物体的范畴。

关键词：中国；区分原则；网络空间；网络战斗员；军事目标；数据。

* 黄志雄是一名来自武汉大学国际法研究所和武汉大学网络治理研究院的教育部青年长江学者，也是华东政法大学“一带一路”建设法律保障机制研究重点创新团队研究员。邮箱：fxyhzx@whu.edu.cn。应瑶慧是一名武汉大学法学院博士研究生，邮箱：yingyaohui@whu.edu.cn。此项研究由国家社科基金重大项目支持（基金编号：20&ZD204）。作者感谢所有编辑和匿名审稿人的有用建议，并感谢埃里克·詹森（Eric Jensen）、库博·马察克（Kubo Mačák）、伊格纳西奥·德拉拉西利亚·德尔莫拉尔（Ignacio de la Rasilla del Moral）、苏金远（Jinyuan Su）、妮科尔·霍格（Nicole Hogg）和尼古拉斯·察古里亚斯（Nicholas Tsagourias）对本文早期草稿的有益评论。本文初稿提交给杨百翰大学 2019 年 2 月举办的“当今混合武装冲突中的法律”研讨会，诚挚感谢与会者的所有反馈和评议。

** 中南财经政法大学法学院国际法系讲师，邮箱：yingyaohui@zuel.edu.cn。

引言

截至目前，中国政府对国际人道法（IHL）[1]在网络空间的适用还不明确。在中国学者中，[2]特别是有军事背景的学者[3]中，对于国际人道法在网络空间中的适用有一些初步的争论，但对网络空间区分原则的讨论在篇幅和学术深度上都很有限。与西方相比，中国学者对该问题的研究还尚处于比较初级的阶段，一些关于国际人道法适用于网络空间的博士论文正在撰写中。目前，中国学术界还没有对区分原则在网络空间中的适用进行具体的解构或澄清。

作为第一篇由中国学者专门研究区分原则在网络战争中适用的论文，本文通过将中国官方立场和中国学者的观点注入到讨论中，提供了一个不同的视角。作者认为，尽管各国对国际人道法在网络空间具体适用的解释有很大差异，但核心的区分原则肯定适用于网络空间。本文旨在澄清现有规则在网络战中是否仍然完全适用，并在需要时找出可以进行何种改进和澄清。因此，第一部分介绍了国际人道法在网络空间的适用现状，并阐述了中国官方在该问题上的态度和中国学界观点。随后，第二部分回顾了区分原则的概念并指出了其在网络背景中适用的争议性挑战。应用人/物二分法，第三和第四部分考察了涉及的实质性法律挑战，并注入了相关的中国观点。从人类目标的角度，第三部分分析了网络战场上界定谁可以被攻击的传统标准的应用，识别了相关障碍并提出了相应的建议。第四部分聚焦于非人类目标并讨论了在网络战中什么可以被攻击——即什么构成了军事目标。它进一步涉及了中国学者关于数字数据本身是否构成物体的问题。最后一部分提出了一些初步的结论性意见。

毫无疑问，和平利用网络空间对人类的共同福祉具有重要意义。幸运的是，迄今为止，世界上还没有发生任何灾难性的大规模伤亡网络攻击，也没有发生类似“网络珍珠港”[4]事件这样的战争

---

[1] 为了避免混淆，在此谨提醒以澄清两个术语，“武装冲突法（LOAC）”和“国际人道法（IHL）”。有人担心这两个术语的不准确使用。有人认为它们本质上是相同的意思并可互换使用，例如，“武装冲突法，又称国际人道法，包括区分军事目标和民用目标等原则”（International Committee of the Red Cross (ICRC), *The Law of Armed Conflict: Basic Knowledge*, Geneva, June 2002, p. 2, available at: www.icrc.org/eng/assets/files/other/law1_final.pdf），而另一些人则认为“国际人道法”是一个可能比较狭义的概念，只涉及武装冲突中的法律，这些法律旨在规范武装冲突中的人——平民或军人、伤员或现役人员——的待遇（Mary O’Connell, “Historical Development and Legal Basis”, in Dieter Fleck (ed.), *The Handbook of International Humanitarian Law*, 3rd ed., Oxford University Press, Oxford, 2013, p. 11）。也有人对战场法和人道主义目标的融合提出了一些批评，例如，“〔国际人道法〕一词的一个可能的缺点是，它可被认为排除了首要目的不是人道主义的战争法的某些部分（如中立法）”（Jean Pictet, *Humanitarian Law and the Protection of War Victims*, A. W. Sijthoff, Leiden, 1975, p. 11）。国际法委员会对武装冲突法和国际人道法进行了区分，前者规制武装冲突的行为和后果，而后者则是前者的一部分，构成规制敌对行动的特别法（para. 4 of the Commentary to Art. 2 of the Draft Articles on the Effects of Armed Conflicts on Treaties, *ILC Yearbook*, Vol. 2, Part 2, 2011）。有关术语的更详细讨论，见 Gary D. Solis, *The Law of Armed Conflict: International Humanitarian Law in War*, Cambridge University Press, Cambridge and New York, 2010, pp. 22–26。中国的教科书和论文普遍认为，“国际人道法”的术语是由“战争法”或“武装冲突法”演变而来，故将其视为同义词；例如，见朱文奇：《何谓“国际人道法”》，《武大国际法评论》2003 年第 1 期。为本文的目的，“国际人道法”一词将被作一般使用，而“武装冲突法”一词则在所引用资料来源使用该特定术语时使用。

[2] 例如，见张力：《网络战的中国视角》，《红十字国际评论》，第 94 卷，第 886 期，2012 年，第 244 页，载：https://international-review.icrc.org/zh-hans/articles/chinese-perspective-cyber-war（所有互联网参考资料都在 2021 年 1 月最后访问）；Longdi Xu, “The Applicability of the Laws of War to Cyberspace: Exploration and Contention”, 2014, p. 7, available at: www.gov.uk/government/publications/the-applicability-of-the-laws-of-war-to-cyberspace-exploration-and-contention; Chris Wu, “An Overview of the Research and Development of Information Warfare in China”, in Edward Halpin, Philippa Trevorrow, David Webb and Steve Wright (eds), *Cyberwar, Netwar and the Revolution in Military Affairs*, Palgrave Macmillan, London, 2006; 朱莉欣：《信息网络战的国际法问题研究》，《河北法学》2009 年第 1 期；姜世波：《网络攻击与战争法的适用》，《武大国际法评论》2013 年第 2 期第 16 卷；李伯军：《论网络战及战争法的适用问题》，《法学评论》2013 年第 4 期；朱莉欣：《平战结合与网络空间国际规则制定》，《信息安全与通信保密》2018 年第 7 期。

[3] 王海平：《武装冲突法研究进展及需要关注的问题》，《当代法学》2012 年第 5 期；李莉、鲁笑英：《浅析信息化战争条件下武装冲突法所面临的问题》，《西安政治学院学报》2012 年第 1 期；朱雁新：《计算机网络攻击之国际法问题研究》，中国政法大学博士论文，2011 年；张天舒：《从“塔林手册”看网络战争对国际法的挑战》，《西安政治学院学报》2014 年第 1 期。

[4] James J. Wirtz, “The Cyber Pearl Harbor”, *Intelligence and National Security*, Vol. 32, No. 6, 2017; James J. Wirtz, “The

催化剂。然而，令人不安的网络交战事件层出不穷，如将网络手段和方法纳入武装冲突，迫使我们密切关注国际人道法在网络空间的适用。

网络战，[5]尽管有可能允许在特定的基础上实现某种程度的匿名和相互联系，但它仍然是一种战争。因此，关于国际人道法——“旨在限制武装冲突影响的一套规则”[6]——是否适用于网络空间领域的多边讨论已经进行了十多年。目前尚未达成共识。2014/15 年联合国关于从国际安全的角度看信息和电信领域的发展的政府专家组报告似乎有一丝希望，因为该报告已经提到了区分原则和比例原则在网络空间的可适用性：[7]“国际法律原则，包括……区分原则”[8]的措辞被视为一种妥协，因为一些国家（可能包括中国）不希望直接提及国际人道法一词。[9]然而，随后的 2016/17 年联合国政府专家组未能达成共识，其中一个有争议的问题就涉及国际人道法在网络空间的适用。[10]随着 2018 年联大第一委员会[11]通过两项分别的（有些人可能会说相互竞争的）决议，各国在网络空间就国际人道法达成共识的前景似乎愈加不确定和令人困惑。

在理想世界里，一旦局势达到武装冲突的门槛，战时法规则在网络空间的适用只不过是新瓶装旧酒。如果网络战仅仅是一种新的作战手段或方法，那么现有的战时法规则将自动适用，这没有什么神秘或不可思议的。然而，现实往往与理想背道而驰。由于网络战场与传统战场的巨大差异，许多现有规则在网络战中显得相当混乱，必须重新赋予概念。在区分原则的情况下尤其如此。例如，与该原则有关的一个重要问题是区分网络战斗员和平民。战斗员有义务公开携带武器或备有可从远处识别之固定的特殊标志。[12]这在网络背景下显然是不现实的，因为在网络环境下，匿名是常态，且不可能知道谁坐在正在实施攻击的计算机前。在这些规则起草的时代，交战的敌对部队之间有一定程度的物理接近；在大多数情况下，战斗员可以看到彼此，因此可以区分战斗员和非战斗员，敌

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

[5] 在本文中，“网络战”一词被理解为“在武装冲突中使用的依赖于信息技术的作战手段和方法”。See Jakob Kellenberger, “International Humanitarian Law and New Weapon Technologies, 34th Round Table on Current Issues of International Humanitarian Law, Sanremo, Italy, 8–10 September 2011: Keynote Address by Dr Jakob Kellenberger”, *International Review of the Red Cross*, Vol. 94, No. 886, 2012, available at: https://international-review.icrc.org/sites/default/files/irrc-886-kellenberger-spoerri.pdf. 在一些中国学者看来，网络战是一种特殊的信息战形式，且是一种新的作战手段或方法。信息战是指战场敌对方之间为保持自身对信息的获取权、控制权以及使用权而对对方开展的一系列敌对活动，其内涵和外延要比网络战更广，它可以包括网络战、情报战、电子战、心理战等。网络战是指通过计算机网络，扰乱、破坏或威胁其他交战方的信息和网络系统，同时保证己方信息和网络系统安全的过程。例如，见李伯军，前注 2。一些人认为，“网络战”概念所表达的主要问题是：以键盘、鼠标、电脑病毒和其他恶意软件为“武器”的网络攻击，是否可能成为（或已经成为）一种新的战争形态或作战手段。见黄志雄主编：《网络空间国际规则新动向：〈塔林手册 2.0 版〉研究文集》，社会科学文献出版社 2019 年版，第 301 页；黄志雄：《国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心》，《现代法学》2015 年第 5 期。

[6] 见红十字国际委员会，“战争与法律”页面，载：http://www.icrc.org/zh/war-and-law。

[7] 见联合国政府专家组，《关于从国际安全的角度看信息和电信领域的发展政府专家组的报告》，联合国第 A/70/174 号文件，2015 年 7 月 22 日，第 28 段，载：https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/34/PDF/N1522834.pdf?OpenElement。

[8] 同上注。

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

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

[11] See “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased”, *Council on Foreign Relations Blog*, 15 November 2018, available at: www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased. 这两项决议分别由俄罗斯（联合国第 A/C.1/73/L.27/Rev.1 号文件）和美国（联合国第 A/C.1/73/L.37 号文件）提出。

[12]《一九四九年八月十二日关于战俘待遇之日内瓦第三公约》，75 UNTS 135（1950 年 10 月 21 日生效）（《日内瓦第三公约》），第 4 条子款第 2 项；《一九四九年八月十二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》，1125 UNTS 3，1977 年 6 月 8 日（1978 年 12 月 7 日生效）（《第一附加议定书》），第 44 条第 3 款；让-马里·亨克茨和路易丝·多斯瓦尔德-贝克：《习惯国际人道法第一卷：规则》，红十字国际委员会、剑桥大学出版社 2005 年版，中文译本由红十字国际委员会组织编译，红十字国际委员会、法律出版社 2007 年版（简称《红十字国际委员会习惯法研究》），第 13～16 页，载：https://ihl-databases.icrc.org/zh/customary-ihl/v1。

或友。[13]当涉及到直接参加敌对行动的平民时，[14]这个问题就更加令人困惑了。无组织的个人向对手发动网络攻击的可能性很高；典型例子是一群黑客分子出于爱国或意识形态的原因进行分布式拒绝服务（DDoS）攻击。例如，2007 年发生的针对爱沙尼亚基本基础设施、通讯、DNS 服务器、网站和电子邮件服务器的匿名网络攻击，似乎是在一场关于将象征着苏联击败纳粹的苏联“爱沙尼亚解放者纪念碑”从塔林市中心迁至城郊军事公墓的政治争议之后出现。[15]在这一事件中，谁是直接参加敌对行动的人？是输入恶意代码的人，或编写（但不执行）代码的人，抑或最初下令编写代码的人？

作为网民数量最多的国家，也是频频遭受网络攻击的国家之一，[16]中国一直非常积极地推进网络空间法治。然而，尽管中国多年来一直是日内瓦四公约[17]及其两个附加议定书[18]的缔约国，但中国对网络空间的国际人道法问题并无太多热情，也一直对网络战及其法律问题趋于回避。[19]

中国不愿深入讨论国际人道法的问题已经在一些场合找到例证。例如，在最近提交给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的文件中，中国指出“武装冲突法和诉诸战争权的适用问题需要谨慎处理”。[20]这表明，出于某种（可能是政治）原因，中国不愿讨论网络空间国际人道法的细节，因此推迟了对该问题的澄清。中国并未具体说明立场和理由，只是一再申明“网络战的合法性在任何情况下都不应被承认”。[21]这种抗拒的态度在中国代表在 2019 年亚非法律协商组织（AALCO）年会上的发言中表现得比较明显：

> 中国坚持和平利用网络空间的原则，坚决反对……网络战或网络军备竞赛。……在没有国家实践的情况下，我们应该非常谨慎地讨论在所谓的“网络战”中适用人道法。原因很简单但很基本：首先，没有网络战应该被允许；其次，网络战将是一种全新的高科技战争形式。考虑到发展中国家和……发达国家之间的“数字鸿沟”，总体来说发展中国家在讨论和制定这些规则时将处于不利地位，〔而且〕很难确保这些规则是公平和公正的。[22]

中国高度重视和平利用网络空间，认为过多讨论国际人道法适用问题可能对国际和平与安全产生负面影响，加剧网络空间军备竞赛和军事化。例如，中国批评这种“军事范式”[23]无视禁止使用

---

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

[14] 《红十字国际委员会习惯法研究》，前注 12，规则 6，规定应保护平民免遭攻击，除非他们正在直接参与敌对行动。关于“直接参加敌对行动”的实质性讨论，见尼尔斯·梅尔泽，《国际人道法中直接参加敌对行动定义的解释性指南》，红十字国际委员会，2009 年（《解释性指南》）。

[15] 关于 2007 年针对爱沙尼亚的网络攻击的详细描述，见“Cyber Attacks against Estonia (2007)”, *International Cyber Law in Practice: Interactive Toolkit*, NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), available at: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007); Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations*, CCD COE, Tallinn, 2010, pp. 15–16, 31.

[16] Chinese Academy of Cyberspace Studies (ed.), *China Internet Development Report 2017*, Springer, Berlin, 2019, p. 107; 国家互联网应急中心，《2020 年上半年我国互联网网络安全监测数据分析报告》，2020 年，载：https://www.cert.org.cn/publish/main/upload/File/2020Report(2).pdf；中华人民共和国外交部，《2020 年 9 月 29 日外交部发言人汪文斌主持例行记者会》，载：https://www.mfa.gov.cn/web/wjdt_674879/zcjd/202009/t20200929_7943814.shtml。

[17] 中国批准/加入日内瓦四公约的日期是 1956 年 12 月 28 日。见红十字国际委员会条约数据库，载：https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=CN。

[18] 中国批准/加入《第一附加议定书》和《第二附加议定书》的日期为 1983 年 9 月 14 日。同上注。

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

[20] See “China’s Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security”, p. 6, available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

[21] *Ibid*.

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

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

武力的原则，[24]可能影响国家间的战略互信，增加国家间产生误解和冲突的风险。[25]在这种背景下，中国政府对区分原则在网络空间的适用态度不明确就不足为奇了。中国的保守态度在一定程度上是可以理解的。首先，没有公认的能够构成网络攻击的国家实践；其次，由于法律本质上的滞后性，网络空间的国际人道法不应被太早确定。[26]中国政府目前对这一问题的现有保守态度，也可能是在中国还没有拿出一个自圆其说的方案的情况下采取的拖延策略。笔者认为，国际人道法在网络空间的适用，特别是区别原则，不存在法律上的障碍。不可否认，网络战已经发生并将继续发生。不管中国喜欢与否，它可能都不得不表明自己对网络空间国际人道法的立场。

区分原则与将其适用到网络空间的挑战

在介绍了国际人道法在网络空间的适用现状、中国的官方态度以及一些中国学者对此的见解之后，现在是时候回顾区分原则本身，并总结其在网络背景中适用的有争议的挑战了。根据国际法院在其《以核武器相威胁或使用核武器的合法性》的咨询意见，区分原则是武装冲突法的一项基本原则，并已取得习惯国际法的地位。[27]《第一附加议定书》第 48 条规定，冲突各方无论何时均应在平民居民和战斗员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。[28]

总体来说，区分原则对规范敌对行动采取了一种双管齐下的方式。它禁止不分皂白的作战方法和手段，并对合法作战方法和手段的使用进行规制——这意味着一方面要区分军事目标和战斗员，另一方面要尊重和保护其他人员和物体。不分皂白的攻击是被禁止的。[29]

“攻击”引发了一系列有关区分的法律保护，尤其是《第一附加议定书》第 49～58 条中所包含的内容。因此，为了澄清区分原则究竟如何能够适用于网络空间，对“网络攻击”的适合定义是一个先决条件。关于什么会构成网络攻击，目前已经累积了一些深入而有意义的学术讨论。[30]最广泛接受的定义采用了一种基于结果的方法。例如，《网络行动国际法塔林手册 2.0 版》（《塔林手册 2.0 版》）将网络攻击定义为“无论进攻还是防御，网络攻击是可合理预见的会导致人员伤亡或物体损毁的网络行动”。[31]我们在本文中采纳该定义。[32]没有明显的法律规定明确禁止或规制网络战的使用，这与其他形式的战争不同。国际人道法目前对网络战中的区分问题保持沉默，一些学者因此

---

[24] Xinmin Ma, “What Kind of Internet Order Do We Need?”, *Chinese Journal of International Law*, Vol. 14, No. 2, 2015. 马新民在 2014 年至 2019 年间任外交部条法司副司长。

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

[26] 更多关于中国对国际人道法态度的解释，见 B. Zhang, above note 19。

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

[28] 《第一附加议定书》第 48 条；《红十字国际委员会习惯法研究》，前注 12，规则 1 和规则 7，第 3 页和第 24 页。

[29] 《第一附加议定书》第 51 条第 4 款；《红十字国际委员会习惯法研究》，前注 12，规则 11，第 35 页。

[30] See Marco Rossini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, pp. 178–182; William H. Boothby, “Where Do Cyber Hostilities Fit in the International Law Maze?”, in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict*, Springer, Berlin, 2014, pp. 60–62; Knut Dörmann, “Applicability of the Additional Protocols to Computer Network Attacks”, paper presented at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17–19 November 2004; 克尔杜拉·德勒格，《别碰我的云：网络战、国际人道法与平民保护》，《红十字国际评论》，第 94 卷，第 886 期，2012 年；Michael N. Schmitt, “The Law of Cyber Warfare: Quo Vadis?”, *Stanford Law and Policy Review*, Vol. 25, No. 2, 2014.

[31] 迈克尔·施密特（Michael Schmitt）总主编，《网络行动国际法塔林手册 2.0 版》，剑桥大学出版社 2017 年版，中文译本由黄志雄等译，社会科学文献出版社 2017 年版（《塔林手册 2.0 版》）规则 92，第 406 页。

[32] 基于结果的方法非常有用，因为它将焦点从行为的手段和性质转移到行为的效果和结果上，从而满足了“暴力”的要求，保持了该条文的动态和演进。然而，笔者仍然有两处关切。首先，从实际角度来看，对损失的评估是非常棘手的，尤其是当后果大多是间接的。第二个关切是，基于结果的方法限制了攻击的概念，从而排除了那些造成严重和破坏性非物理损害的行动。类似的担忧可见于红十字国际委员会，《国际人道法与武装冲突中的网络行动》，日内瓦，2019 年 11 月（《红十字国际委员会网络行动文件》），第 7 页。红十字国际委员会还提到，对攻击概念过度严格的解释，难以与保护平民居民和民用物体免受敌对行动影响的敌对行动规则的目的和宗旨相一致。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》，32IC/15/11，2015 年 10 月（《红十字国际委员会 2015 年挑战报告》），第 40 页。

认为，现有基于条约的框架不适合应对网络战；虚拟战争的这一方面对区分原则的适用产生了负面影响。[33]这其中的一个原因，正如一些学者指出，[34]是民用和军事基础设施不仅密切相关和相互联系，并且实际上就是同一件事。这种主张可能得出对区分原则之适用构成重大障碍的结论。如果网络空间的大多数组成部分——如光纤电缆、卫星、路由器和节点——都是军民两用物体，同时服务于军事和民用目的，那么对这些物体的分类可能会存在困难，导致有关比例原则的棘手问题。[35]与此同时，由于战争平民化现象的不断增加，[36]其特点是越来越多地使用复杂的网络技术，这种现象模糊了战争的轮廓，因而将个人划分为战斗员或平民的界限并不总是很清楚。军民企业的交流、合作和融合也达到了前所未有的深度。[37]例如，中国曾两次将军民融合战略纳入其白皮书。[38]此外，责任的归因也存在困难；[39]虽然通常很容易看到导弹是从哪里发射的，但网络行动的部署则不会产生烟尘。

一些学者对区分原则在网络战中的适用进行了缜密研究，[40]美国[41]和丹麦[42]等一些国家在各自的《军事手册》中增加了区分原则在网络战中适用的内容。例如，人们普遍认为，攻击不一定必须是动能的才可让国际人道法规则适用；禁止不分皂白的攻击；[43]如果攻击没有明确针对任何特定的军事人员或物体，就永远不应被允许。如果计算机病毒能从军事系统不受控制地传播到与之相连的民用系统，就可能出现这种情况。虽然对于必须区分军事目标/战斗员和民用物体/平民已存在共识，但当涉及到更实际的层面，即什么构成军事目标以及谁是网络武装冲突中的战斗员时，这个问题变得极富争议。此外，正如一位中国学者所提出的，网络方法和手段的非致命的底层特征使得传统受保护的物体和个人在网络战中比在常规战争中更加脆弱。这将导致网络行动正当性评估的混乱，使区分原则在网络军事行动中更容易被违反。[44]鉴于区分原则在网络战场上的重要意义，有必要澄清现有规则在网络战中是否仍然完全可适用，以及在哪些方面可以进行改进和澄清。

网络战中有关人类目标的区分原则

区分原则遵循人/物二分法来界定目标的性质。无论网络技术如何发展，恶意行为的实施者仍然是人，即使在植入病毒或攻击防火墙时，看起来（实施者）只是敲击键盘和点击鼠标，这种界定“谁”和“什么”可以被攻击的人/物二分法也仍然适用。本文的这一部分将讨论在网络背景中谁

[33] See Jeffrey Kelsey, “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare”, *Michigan Law Review*, Vol. 106, No. 7, 2008, pp. 1429–1430.
[34] Robin Geiss and Henning Lahmann, “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space”, *Israel Law Review*, Vol. 45, No. 3, 2012, pp. 381, 383.
[35] 区分原则规定，在武装冲突中只能直接针对军事目标。但是，对合法军事目标的攻击有时可能对平民或物体造成附带损害。这些有害的副作用受到比例原则的规范，该原则禁止可能对平民生命或财产造成与预期的具体和直接军事利益相比损害过分的攻击。对比例原则的明确表述见《第一附加议定书》第 51 条第 5 款第 2 项。See also Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law*, Edward Elgar, Cheltenham, 2013, pp. 55–57.
[36] “平民在武装冲突中扮演着越来越重要和复杂的角色，既是受害者也是实施者。”这一整体趋势被称为“平民化”，见 Andreas Wenger and Simon J. A. Mason, “The Civilianization of Armed Conflict: Trends and Implications”, *International Review of Red Cross*, Vol. 90, No. 872, 2008。
[37] 朱莉欣，《平战结合与网络空间国际规则制定》，前注 2，第 40 页。
[38] 国务院新闻办公室，《新时代的中国国防》，北京，2019 年 7 月，载：http://www.scio.gov.cn/ztk/dtzt/39912/41132/41134/Document/1660318/1660318.htm；国务院新闻办公室，《中国的军事战略》，北京，2015 年 5 月，载：http://www.scio.gov.cn/gxzt/dtzt/2015_22766/2015ngzhg/zfbps_23174/202209/t20220920_399870.html.
[39] 见《红十字国际委员会网络行动文件》，前注 32，第 8 页。
[40] See, for example, J. Kelsey, above note 33, p. 1427; Yoram Dinstein, “The Principle of Distinction and Cyber War in International Armed Conflicts”, *Journal of Conflict and Security Law*, Vol. 17, No. 2, 2012, p. 261; Michael N. Schmitt, “Wired Warfare: Computer Network Attack and Jus in Bello”, *International Review of the Red Cross*, Vol. 84, No. 846, 2002, p. 365.
[41] DoD, *Law of War Manual*, Washington, DC, 12 June 2015, pp. 985–999.
[42] Danish Ministry of Defence, Defence Command Denmark, *Military Manual on International Law Relevant to Danish Armed Forces in International Operations*, Copenhagen, September 2016.
[43] 《第一附加议定书》第 51 条第 4 款。
[44] 陈鹏飞，《论当代武装冲突法面临的挑战》，《西安政治学院学报》2014 年第 5 期。

可以被合法攻击的问题。基本原则是平民不应成为攻击的对象。[45]区分原则假定交战各方能够清楚地区分平民和战斗员；然而，网络空间的匿名属性使得这种推定难以维持。

每一名战斗员都曾是平民，任何平民都可能将自己转变为战斗员，[46]或通过被征召或自愿加入交战一方的武装部队，或通过直接参加敌对行动（这导致在此期间内失去受保护的地位），[47]或通过成为民众抵抗的一员，这一概念（即民众抵抗）允许从平民过渡到合法的战斗员。[48]作者不会在这里讨论民众抵抗，因为这一概念需要对国家领土的实际入侵和大量人口的参与，[49]而通过网络手段这几乎是不可能的。[50]

由于容易否认国家责任和成本低的优点，“大多数网络行动都外包给平民网络专家”。[51]根据这一趋势，除纳入正规武装部队的网军外，“实质性参与网络行动的许多人员实际上会是平民”的可能性很大。[52]爱国的黑客或计算机科学家可以因此成为攻击的对象吗？答案取决于在网络行动背景下对“直接参加敌对行动”的理解。

谁是网络战斗员?

直接参加敌对行动的平民会失去受保护地位，并且也无权享受战斗员豁免；一些学者甚至认为他们是“非法”[53]战斗员。国际人道法鼓励明确和可靠地划分战斗员和非战斗员，这反映了区分原则在这一法律体系中发挥的根本作用。战斗员有权直接参加敌对行动，[54]并因此免于因实施符合国际人道法的行为而被起诉；[55]所以，他们是可攻击的目标。这在网络战中也不例外。由于平民的定义是一个纯粹的负面定义（平民是属于非战斗员的人[56]），谁是网络战斗员的问题就成为一个关键问题。[57]

已经看到，一些国家在其武装部队中设立了负责网络行动的特别部门。例如，美国建立了美国网络司令部（US CYBERCOM），它从美国战略司令部的一个下属单位提升到统一作战司令部的地位；[58]而哥伦比亚建立了武装部队联合网络司令部，负责预防和打击影响国家价值和利益的网络威胁或攻击。[59]网络战斗员的定义是值得讨论的，因为它不仅涉及谁是合法目标的问题，而且还会影响到谁在被俘后有权获得战俘（PoW）地位。

---

[45] 《第一附加议定书》第 51 条第 2 款；《红十字国际委员会习惯法研究》，前注 12，规则 6，第 19～23 页。

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

[47] 《第一附加议定书》第 51 条第 3 款；《红十字国际委员会习惯法研究》，前注 12，规则 6，第 19～20 页；《解释性指南》，前注 14，第 39～66 页。

[48] 《日内瓦第三公约》，第 4 条子款第 6 项；《红十字国际委员会习惯法研究》，前注 12，规则 106，第 367 页，以及特别是规则 5，它解释了民众抵抗的成员是平民定义的一个例外，因为尽管他们不是武装部队的成员，但他们有资格成为战斗员。

[49] 《日内瓦第三公约》第 4 条子款第 6 项。

[50] 《塔林手册 2.0 版》，前注 31，规则 88，第 401 页。

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

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

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

[54] 《第一附加议定书》第 43 条第 2 款。

[55] H. Harrison Dinniss, “Participants in Conflict”, above note 13, p. 254.

[56] 《第一附加议定书》第 50 条第 1 款；《红十字国际委员会习惯法研究》，前注 12，规则 5，第 16～18 页。

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

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

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

战斗员基本上是交战一方武装部队的成员——不论这些部队是正规部队还是非正规部队，不论属于常备军还是预备役部队——包括事实上编入武装部队的准军事民兵。在军事机构中分配给个人的具体任务是无关紧要的。[60]

日内瓦四公约列举了合法战斗员地位必须满足的五个条件。[61]前四项是《海牙条例》和日内瓦四公约规定的适用战俘和合法战斗人员身份的累积条件：（甲）有一为其部下负责之人统率（组织）；（乙）备有可从远处识别之固定的特殊标志；（丙）公开携带武器；（丁）遵守战争法规及惯例进行战斗。[62]这四个条件适用于其他民兵及其他志愿部队人员，但它们也是对冲突一方武装部队人员的隐含要求。日内瓦四公约还暗示了一个附加条件，即（戊）属于冲突一方。[63]

作者认为要素（甲）（丁）和（戊）是实质性要素，要素（乙）和（丙）是形式要素。考虑到在网络战争中匿名是常态，把重点放在实质性要素而非形式要素上更有意义。

第一个要素是组织，这在网络战中是必不可少的。这其实更多的是一个事实问题而非法律问题，且该要求反映了负责任的指挥和等级关系的存在。[64]如果一个网络团体没有足够的组织程度，通常是上下级结构、职权和责任分工以及纪律和监督的某些要素，其成员就不能成为合法的战斗员，当然也就无权享有战斗员豁免权。考虑到大多数网络组织的成员都有相同的意图，但缺乏共同的纪律，一个只存在于网络上的武装团体充分组织起来的可能性非常小。[65]例如，如果一个团体的成员突然决定停止或不参加网络敌对行动（可能是网络团体的成员间彼此完全不认识的情况），或者一个团体的成员觉得没有必要遵守指挥官的命令，也并不会产生任何后果，那么认为这样一个组织松散的团体满足了组织要素就是不合理的。这在爱国网络团体中尤其如此。[66]

第四个要素，即遵守国际人道法，仍然是必不可少的且并没有随着计算机网络技术的出现而明显改变。[67]如果战斗员本身不愿尊重国际人道法，他们就无法在希望获得其利益时依靠该法律。[68]

最后一个要素是属于冲突的一方，目的是证明发起网络攻击的团体与交战国之间存在某种联系。[69]虽然计算机网络攻击使“网络民兵”得以使用，并为一国提供了“貌似合理的推诿”的吸引力，但除非该团体与国家之间能够建立联系，否则参加者不会被视为合法战斗员。[70]国家的正规武装部队不需要证明这种联系，但就有组织的网络团体而言，尚不清楚需要对他们进行多大程度的控制。[71]

---

[60] Y. Dinstein, above note 46, p. 41.
[61] H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 144.
[62] 《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》，75 UNTS 31（1950 年 10 月 21 日生效）（《日内瓦第一公约》），第 13 条第 2 款；《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》，75 UNTS 85（1950 年 10 月 21 日生效）（《日内瓦第二公约》），第 13 条第 2 款；《日内瓦第三公约》第 4 条子款第 2 项；《一九四九年八月十二日关于战时保护平民之日内瓦公约》，75 UNTS 287（1950 年 10 月 21 日生效）（《日内瓦第四公约》），第 4 条第 2 款；H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 145.
[63] 《日内瓦第三公约》第 4 条子款第 6 项；H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 145.
[64] Y. Dinstein, above note 46, p. 39; International Criminal Tribunal for Rwanda (ICTR), *The Prosecutor v. Jean-Paul Akayesu*, Case No. ICTR-96-4-T, Judgment (Trial Chamber), 2 September 1998, para. 626.
[65] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014, p. 195.
[66] Tilman Rodenhäuser, *Organizing Rebellion: Non-State Armed Groups under International Humanitarian Law, Human Rights Law, and International Criminal Law*, Oxford University Press, Oxford, 2018, pp. 104–108.
[67] H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 149.
[68] Y. Dinstein, above note 46, p. 54.
[69] See Denise Bindschedler-Robert, “A Reconsideration of the Law of Armed Conflicts”, in *The Law of Armed Conflicts: Report of the Conference on Contemporary Problems of the Law of Armed Conflict*, 1971, p. 40; Katherine Del Mar, “The Requirement of ‘Belonging’ under International Humanitarian Law”, *European Journal of International Law*, Vol. 21, No. 1, 2010.
[70] H. Harrison Dinniss, “Participants in Conflict”, above note 13, p. 262.
[71] 国际法院在尼加拉瓜案中阐述的有效控制标准似乎不适合定义“属于冲突一方”的含义，因为与全面控制和完全依赖标准不同，它表达的是对行为的控制，而不是对行为者的控制，因此着重于具体活动。Marko Milanović, ‘State Responsibility for Acts of Non-state Actors: A Comment on Griebel and Plücken’, *Leiden Journal of International Law* Vol. 22, No. 2, 2009, p. 317. 关于有效控制、全面控制的含义和完全依赖标准，见 Antonio Cassese, The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, *European Journal of International Law*, Vol. 18 No. 4, 2007。

最令人困惑的问题是第二和第三个要素，这两个要素要求战斗员备有可从远处识别之固定的特殊标志，并公开携带武器。这两项条件同在战斗员和平民之间作出区分的原则密切相关。考虑到这两个条件是为了消除这方面的混乱，并排除任何欺骗的企图，[72]将它们移植到在线环境中存在固有困难，因为由于网络空间的匿名性，我们不可能知道是谁坐在任何一台电脑前。有学者提出，鉴于计算机用户不可能被标记可识别的标识，应将展示标识的要求适用于计算机或系统，就像军用汽车、飞机和船舶需要标记有特殊标识一样。这一提议是站不住脚的，因为给军用计算机打上标记就等于使它所连接的任何系统成为合法的目标。[73]

有人可能会争辩说，武装部队仍然可以穿制服，以履行备有可从远处识别之固定的特殊标志的义务；[74]例如，要求美国网络司令部的成员在执行网络行动时穿军装。这一意见显然有可取之处——如果正规军能够穿制服或以其他方式将自己与平民区分开来，那将是最理想的——但在实践中，这种要求可能意义不大，因为交战各方都是匿名状态。这一规定的目的和宗旨是，通过穿制服来消除在区分平民和战斗员方面造成混淆的可能性。在传统的武装冲突中，通过穿制服，在大多数情况下可以清楚地看出谁是战斗员而谁不是。[75]但是，当网络战斗员坐在电脑前，有时距离被攻击者很远时，他（她）们穿不穿制服对其他交战国来说没有区别。无论如何，即使我们坚持认为正式军队应着制服，但在处理网络民兵、志愿部队人员或其他有组织的网络团体时，这一要求是荒谬的。更重要的是，网络空间似乎没有给公开携带武器的要求留下任何空间。定义网络武器已经够困难了，公开携带网络武器更是不切实际。[76]当然，不能忽视的是，确实存在对网络战斗员进行动能攻击的可能性。总之，我们认为在网络战中，第二和第三个要素不会被完全删除，但几乎没有必要对它们进行过多讨论。

有人可能认为，在数字战场上并不真正需要这种区分；在针对军事资产的网络攻击中，实施攻击的人要么是战斗员，要么是直接参加敌对行动的平民。不论哪种情况，这个特定的人都失去了他或她的受保护地位。然而，仍然存在一些问题，特别是他或她一旦被俘是否可享有战俘地位。[77]此外，平民攻击者可能无法满足“损害下限”和“交战联系”的要求，[78]因此他或她根本不会失去受保护地位。

总之，对大多数国家来说，界定谁是网络战斗员不仅是一个复杂的法律问题，而且是一个极其困难的技术问题。现实情况是，目前没有办法明确识别网络战斗员，因此现有规则的适用范围着实有限。与传统武装冲突相比，平民更有可能卷入网络武装冲突。[79]正如迈克尔·施密特所指出的，大量平民涌现（在网络战场）的原因是多方面的。从成本效益的角度来看，对大多数国家来说，训练具有网络攻击和防御专业知识的军事人员是极其昂贵和耗时的，更重要的是，结果并得不到保证。此外，网络技术，就其本质而言，是无法被标准化和量化的。技术不仅总是在发展和升级，而且也太有限和专业化了。[80]

上文提到的（乙）和（丙）项要素——备有可从远处识别之固定的特殊标志，和公开携带武器——不太适合网络背景，因此在网络战中可能不需要考虑。然而，一个人仍然必须至少满足（甲）（丁）和（戊）项要素——有负责任的指挥和等级关系、按照战争法和习惯采取行动，并属于冲突

[72] Y. Dinstein, above note 46, p. 37.
[73] 数以百万计的软件机器人不断地搜索互联网，试图找到连接的计算机；搜索军方指定 IP 地址的机器人可以在几分钟内找到它们。一旦发现，有效地将计算机或系统移出范围的唯一方法是断开连接，这一解决方案很可能破坏其正常运行和/或用途；因此，任何以任何方式保持与网络连接的系统都将完全依赖其电子防御系统来防止和抵御入侵。因此，虽然最初在计算机或系统上显示标识的想法似乎是一个有用的解决方案，但在实践中，它造成了显示标识的目的要求和军队进行行动的能力之间的不平衡。See H. Harrison Dinniss, “Participants in Conflict”, above note 13, p. 257; H. Harrison Dinniss, *Cyber Warfare*, above note 13, pp. 145–149.
[74] 《塔林手册 2.0 版》，前注 31，规则 87，第 397 页。
[75] 情况并非总是如此；例如，直接参加敌对行动的平民可能会受到攻击，但他们几乎不可能身穿军装。
[76] See Prashant Mali, “Defining Cyber Weapon in Context of Technology and Law”, in Information Management Association, *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, IGI Global, Hershey, PA, 2019; Jeffrey T. Biller and Michael N. Schmitt, “Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare”, *International Law Studies*, Vol. 95, 2019; H. Harrison Dinniss, *Cyber Warfare*, above note 13, pp. 250–278.
[77] H. Harrison Dinniss, *Cyber Warfare*, above note 13, p. 148.
[78] 《解释性指南》，前注 14，第 44 页。
[79] 朱莉欣，《平战结合与网络空间国际规则制定》，前注 2，第 40 页。
[80] M. N. Schmitt, above note 52, p. 527.

一方——才能成为合法的战斗员。否则，他们要么仍受保护不受攻击，要么被视为直接参加敌对行动。在这种情况下，当务之急是防止过度军事化和尽量减少对平民的不必要伤害。与此同时，我们应该记住，如果对一个人是否属于平民有疑问，那个人应被推定是平民。[81]因此，过于宽泛地解释网络战斗员的定义将是不道德和非法的。

直接参加敌对行动的平民

与战斗员不同，平民无权直接参加敌对行动；那些这样做的人失去了免受军事行动危险的一般保护，在这样做的期间可能会受到攻击。[82]此外，他们可能会因其行为在国内法院受到起诉，即使其行为在国际人道法下是合法的。[83]在网络背景下，考虑到武装部队将需要网络专业知识的专家工作外包给平民的当前趋势，直接参加敌对行动的平民的概念可能日趋重要。[84]

如前所述，“直接参加敌对行动”一词指的是这样一种概念，即作为一般规则，平民除直接参加敌对行动并在直接参加敌对行动时外，不应成为攻击的目标。[85]这也被称为非战斗员豁免规则。[86]在讨论《第一附加议定书》第 51 条时，各国并未对“直接参加敌对行动”一词的含义作出准确定义。[87]“定点清除”（*Targeted Killings*）案[88]和红十字国际委员会（ICRC）的《国际人道法中直接参加敌对行动定义的解释性指南》（《解释性指南》）[89]都对解释直接参加敌对行动的概念作出了重要贡献。《解释性指南》引发了相当大的争论和一些争议。[90]虽然不确定性仍然存在，并且目前如何在物理战场上适用该指南尚不完全清楚，但在虚拟战场上更是如此。[91]

确定直接参加敌对行动已经相当复杂；确定直接参加网络敌对行动似乎更难。正如“定点清除”案所指出的那样，在完全不使用任何武器的情况下参加敌对行动是可能的。[92]因此，虽然今天的战争手段可能与上个世纪的战争手段有很大不同，但这种战争手段的效果基本上是相似的。军事通信系统无论被计算机病毒损毁，还是被轰炸袭击所破坏，都会同样地不可运转。

为了进一步解构这个问题并为实践者提供指导，《解释性指南》提出了三个叠加的要素，它们共同构成了直接参加敌对行动的行为。首先，该行为必须很可能对武装冲突一方的军事行动或军事能力造成不利影响，或者致使免受直接攻击之保护的人员死亡、受伤或物体毁损（损害下限）。其次，在该行为与可能因该行为（或该行为作为有机组成部分的协同军事行动）所造成的损害之间必须存在直接的因果关系（直接因果关系）。再次，该行为必须是为了直接造成规定的损害下限，其目的是支持冲突一方并损害另一方（交战联系）。[93]计算机网络攻击和计算机网络刺探也都被论及，并得出“对军用计算机网络的电子干扰——不管是通过计算机网络攻击还是计算机网络刺探以及窃听敌方统帅部或者为实施攻击传送战术目标情报——也可构成直接参加敌对行动”的评估结论。[94]这种三要素的组合标准，侧重于损害下限、直接因果关系和交战联系，为评估一个平民是否和在何种程度上从事了网络战斗员的活动从而应由此失去受保护地位提供了一个有用的起点。[95]这些标准

---

[81] 《第一附加议定书》第 50 条第 1 款；《红十字国际委员会习惯法研究》，前注 12，规则 6，第 22～23 页。
[82] 《第一附加议定书》第 51 条第 3 款。《一九四九年八月十二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》，1125 UNTS 609，1977 年 6 月 8 日（1978 年 12 月 7 日生效）（《第二附加议定书》），第 13 条第 3 款；《红十字国际委员会习惯法研究》，前注 12，规则 6，第 19～23 页。
[83] H. Harrison Dinniss, “Participants in Conflict”, above note 13, p. 258.
[84] D. Turns, above note 52, p. 279.
[85] 《第一附加议定书》第 51 条第 3 款。
[86] Judith G. Gardam, *Non-Combatant Immunity as a Norm of International Law*, Martinus Nijhoff, Dordrecht, 1993.
[87] Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary to the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, Martinus Nijhoff, Dordrecht, 1982, pp. 301–304.
[88] Israel High Court of Justice, *Public Committee against Torture in Israel v. Israel et al*., Case No. HCJ 769/02, Judgment, 11 December 2005 (*Targeted Killings*).
[89] 《解释性指南》，前注 14，第 44 页。
[90] “Forum: Direct Participation in Hostilities: Perspectives on the ICRC Interpretive Guidance”, *New York University Journal of International Law and Politics*, Vol. 42, No. 3, 2010.
[91] D. Turns, above note 52, p. 285.
[92] Israel High Court of Justice, Targeted Killings, above note 88, para. 33.
[93] 《解释性指南》，前注 14，第 44 页。
[94] 同上注，第 46 页。
[95] 这个由三部分组成的标准也在《塔林手册 2.0 版》中被适用于网络战，前注 31，第 419～420 页。

在网络背景下是否被以同样的方式解释，仍是一个悬而未决的问题。

第一个要素，即损害下限，涉及造成人身伤亡或财产破坏的客观可能性。例如，如果 2007 年的爱沙尼亚事件[96]和 2010 年的震网事件[97]都是由国际性武装冲突中的平民所为，我们可以得出爱沙尼亚事件中的网络攻击没有达到损害下限，而在震网事件中攻击则达到了损害下限的结论。对爱沙尼亚网络基础设施的网络攻击造成了大规模的不便，或者说妨碍，因为爱沙尼亚是世界上最“联网”（互联网依赖程度最高）的国家之一。但此次攻击没造成人员伤亡，也没有任何财产被摧毁或损坏；而仅仅造成妨碍，无论多么令人不快，都没有达到损害下限。[98]然而，国际人道法既未对“妨碍”进行定义，也不经常使用该术语。[99]

另一方面，针对伊朗用于铀浓缩的核离心机的网络攻击，对这些离心机造成了物理损坏。[100]在这方面，《塔林手册 2.0 版》规定，“行为……必须意图或事实上已对敌方军事行动或军事能力造成负面影响，或者导致免受直接攻击的人员或物体遭受死亡、物理伤害或物质上的毁灭”。[101]因此，按照该手册所述，即使行为仅仅产生了意图的效果，也达到了损害下限。这一解释将损害要素的门槛从客观可能性扩大到主观意图或客观可能性，并进一步在这一点上留下了很大的自由裁量空间。

第二个要素，直接因果关系，应该进行广义解释。根据《解释性指南》，所述损害必须在“一个因果步骤”中产生。[102]对因果关系接近性的这种严格解释在网络行动中尤其有问题，因为某一特定行为的间接或连锁效应实际上可能正是攻击的目的。我们认为，包含主观和客观两种视角的“近因关系”更适用于网络背景——即客观上，由网络行为造成的损害是该行为正常和自然的后果，且这种损害在主观上是可预见的。[103]

一些假设的场景可以帮助我们更好地理解网络背景中的近因关系标准。受雇从事一般计算机和 IT 服务的平民如果只是履行服务合同，如运行网页和管理电子邮件登录终端，将不会被视为直接参加敌对行动，[104]因为因果关系不是直接的，所造成的任何损害不是所涉行动的正常和自然后果，而且提供服务的人员可能无法预见任何负面后果。另一方面，任何专门受雇进行恶意网络攻击的雇员或承包商一旦进行了此类攻击，在理论上就会满足近因关系的要求。

同样值得尝试的是适用洛克希德·马丁公司的“网络杀伤链”模型，[105]以测试在特定条件下是否存在近因关系。网络杀伤链模型是网络攻击的七个步骤的有序排列，即侦察、武器化、投递、刺探、安装、命令与控制以及目标达成。[106]它给出了黑客如何攻击目标的鸟瞰图，尽管不是每一次攻击都遵循所有这些步骤，但它仍然提供了一个很好的起点。第一阶段是侦察，包括研究、查明和选择目标；接下来是武器化阶段，将恶意软件和漏洞组合成可投递和散布的有效载荷。下一步是投递，包括传输武器到目标（例如，通过 USB 驱动器或电子邮件附件）；随后，该武器将试图刺探一个弱点以接近受害者。在第四阶段结束之前，仍然很难判断行为是否与结果有直接的因果关系，因为接下来发生的事情对实施者来说不一定是可预见的。然而，当涉及到安装、命令与控制以及目标达成阶段时，实施者很有可能能够预见将要发生的事情，所造成的损害是相关行为的自然或正常后果。

---

[96] “Cyber Attacks against Estonia (2007)”, above note 15; E. Tikk, K. Kaska and L. Vihul, above note 15, pp. 14–33.
[97] “Stuxnet (2010)”, *International Cyber Law in Practice: Interactive Toolkit*, CCD COE, available at: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010); E. Tikk, K. Kaska and L. Vihul, above note 15, pp. 66–89.
[98] D. Turns, above note 52, p. 286.
[99] 《红十字国际委员会 2015 年挑战报告》，前注 32，第 40 页。
[100] 一份报告显示，在 2009 年底至 2010 年初期间，伊朗纳坦兹一个燃料浓缩工厂的大约 1000 台离心机必须更换，这意味着这些离心机已经损坏。David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Institute for Science and International Security, 22 December 2010; “Stuxnet (2010)”, above note 97.
[101] 《塔林手册 2.0 版》，前注 31，第 429 页。
[102] 《解释性指南》，前注 14，第 50 页。
[103] Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals,* Cambridge University Press, Cambridge, 1987, p. 181.
[104] See Emily Crawford, *Virtual Battlegrounds: Direct Participation in Cyber Warfare,* Sydney Law School Research Paper No. 12/10, 8 February 2012, available at: https://ssrn.com/abstract=2001794.
[105] See Lockheed Martin, “Gaining the Advantage, Applying Cyber Kill Chain Methodology to Network Defense”, 2015, available at: www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.
[106] *Ibid*.

交战联系要素与其说是法律问题，不如说是事实问题。确实，它要求“行为必须是为了直接造成规定的损害下限，其目的是支持冲突一方并损害另一方”。[107]但这不是主观要件。重要的是行为的目的，它必须客观地被设计为直接造成损害。这导致一种推论，即在胁迫下或在不知情的情况下进行的敌对行动不符合交战联系的要素。鉴于僵尸网络攻击频繁发生的事实，必须指出的是，如果民用计算机被僵尸网络攻击，而相关用户不知晓病毒和攻击，则应不属于失去豁免权的情形。在这种情况下，相关用户不应被视为在执行一项行动，因此，由于缺乏任何行动的表现，他们将不满足交战联系要素。

如果一名平民只是编写了一个会导致关键基础设施关闭的恶意软件程序，这种行为不应被视为直接参加网络敌对行动，因为它通常无法同时满足三个要素，而且在任何情况下，因果关系都太过遥远。近似地，平民科学家和武器专家一般被认为受到保护，不受直接攻击。[108]如果一个平民将这种自己编写的恶意程序发送给他或她支持的武装部队，这种行为仍然不构成直接参与敌对行动——这与运输武器类似。然而，如果该恶意程序旨在进行特定的敌对行为，该行为将成为某网络军事行动的组成部分，从而满足近因的因果关系要求。当一个平民执行这样一个恶意程序，无论他（她）是与武装部队签订合同还是单方行动，则很可能会满足要素从而失去受保护地位，成为合法的目标，至少在程序执行期间是这样。

《第一附加议定书》第 51 条还规定了构成直接参加敌对行动的具体行为的时间范围——即平民在直接参加敌对行动“时”失去免受直接攻击的保护。[109]如果“〔此种〕时〔期〕”已经结束，给予平民的保护就会恢复。这应与为有组织武装团体的武装派别成员和属于冲突一方的成员所制定的规则不同；这些人不再是平民，因此在他们负有持续作战职责期间将失去免受直接攻击之保护，而平民在构成直接参加敌对行动的具体行为期间将失去保护。[110]

在网络背景中，一个特别重要的问题是，在处理相对集中的时间段内重复的网络行动时，如何计算平民失去保护的时间范围。如果一名平民多次发动可能构成直接参加敌对行动的网络行动，该平民成为可攻击目标的时间范围或期间是什么？

在传统的战场环境中，《解释性指南》采取了分别对待这些行动的立场，[111]但“定点清除”案在这方面表达了对“旋转门”现象的关注。[112]在《解释性指南》看来，平民保护的“旋转门”防止了攻击那些在当时不构成军事威胁的平民。[113]由于直接参加敌对行动这一概念指的是具体的敌对行为，因此，每当平民所从事的敌对行为结束时，国际人道法就恢复对其免受直接攻击的保护。[114]考虑到 DDoS 攻击等大量网络攻击会在一段时间内多次进行，这种严格的时间划分在操作上意义有限。然而，作者对从第一次操作到整个间歇活动的周期计算方法也持怀疑态度。这是因为直接参加敌对行动的平民与有组织的军事团体成员不一样：虽然他们都是可攻击的目标，但他们是两种类型的人类目标。如前所述，有组织的军事集团成员在其负有持续作战职责的整个期间都是攻击目标，但直接参加敌对行动的平民只在其具体行为期间是攻击目标。“一次或偶尔直接参加敌对行动的平民，后来从该行动中脱离出来，即从他脱离该行动之时起，有权得到保护，不受攻击。”[115]因此，假设一个平民参加了多次网络攻击，如果整个时间段（从第一次攻击开始到最后一次攻击结束）都被连续计算为该平民可以被攻击的时间段，则在某种意义上，我们是在按照战斗员的标准来对待直接参加敌对行动的平民（持续作战职责），因为我们直接将这段间歇时间也视为可攻击的期间。严格地说，直接参加敌对行动的平民因其具体行为而失去受保护地位，不被认为在间歇期间进行了任何敌

[107]《解释性指南》，前注 14，第 44 页。

[108] ICRC, *Fourth Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report*, Geneva, 27–28 November 2006, p. 48. 本文作者注意到，有人对这种评估在极端情况下是否能够维持表示怀疑，即在某些情况下，某一平民的专门知识对武装冲突的结果具有非常特殊和潜在的决定性价值，例如第二次世界大战期间核武器专家的情况。

[109]《第一附加议定书》第 51 条第 3 款；《红十字国际委员会习惯法研究》，前注 12，规则 6，第 19～23 页。

[110]《解释性指南》，前注 14，第 71 页。

[111]《解释性指南》，前注 14，第 68～69 页。

[112] Israel High Court of Justice, *Targeted Killings*, above note 88, para. 40.

[113]《解释性指南》，前注 14，第 68～69 页。

[114] 关于将直接参加敌对行动描述为可能是“间歇性和不连续的”表述，见 ICTR, *The Prosecutor v. Strugar*, Case No. IT-01-42-A, Judgment (Appeals Chamber), 17 July 2008, para.178。

[115] Supreme Court of Israel, *Public Committee against Torture in Israel v. Government of Israel*, Case No. HCJ769/02, 13 December 2006, para. 39.

对行动。另一方面，如果一个平民加入了军事组织，进行了一连串敌对行动，其间只有短暂的休息，那么他在整个活动期间就都失去了免受攻击的豁免权。对这样的人来说，敌对行动之间的间歇不过是为下一此敌对行动做准备。[116]

综上所述，在解释直接参加敌对行动时，损害下限需要客观可能性而不仅仅是主观的意图，并且必须确认交战联系，而因果关系应该是近因的。时间范围是非常重要的，但很难确定。到目前为止，由于缺乏关于这一问题的国际判例，这一概念的澄清仍然留给学术研究、未来的国家实践和司法判决。

网络战中有关非人类目标的区分原则

所有非人类目标[117]可以被分为两类：军事目标和民用物体。民用物体是指所有不是军事目标的物体。[118]攻击应严格限于军事目标。[119]这一部分将讨论在网络领域适用区分原则时在法律下什么可以被攻击——即在网络背景中什么构成军事目标。令人担忧的是，网络空间中的几乎所有东西都具有巨大的军事潜力，军民两用物体的问题在确定目标方面发挥着比以往任何时候都更重要的作用。随着数据在网络武装冲突中的重要性日益增加，数据本身是否可以被视为军事目标的问题也将被涉及。

“军事目标”的概念：两个同等重要的要素

就所有非人类军事目标而言，被广泛接受的定义如下：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。[120]

“军事目标”的概念是至关重要的，因为它直接决定了根据区分原则什么可以被攻击而什么不能。在现实中，对“军事目标”一词的解释有多种。有人认为，《第一附加议定书》第 52 条第 2 款的定义中是指军事行动的作战能力或维持作战能力，包括“间接但实际支持和维持敌人的作战能力”的目标。[121]实际上，遵守第一个标准“实际贡献”一般会产生第二个标准“明确的军事利益”所要求的利益。[122]另一种观点则认为只有当这两个要素累积存在时，才构成该附加议定书意义上的军事目标。[123]换句话说，对一个物体的军事地位的检验是双重的，并且这两个要素同等重要。[124]

本文作者不同意“实际贡献”包括“间接但实际支持和维持敌人作战能力”的目标，特别是在网络领域。这种解释太过宽泛，并且有悖于军事目标限制背后的哲学考量——事实上，通过将贡献定性为“实际的”，将利益定性为“明确的”，《第一附加议定书》的起草者试图避免对构成军事目标的内容进行如此宽泛的解释。[125]在网络战的背景下，这种宽泛的解释会使区分更加混乱；[126]鉴于在网络空间中几乎所有东西都具有军事潜力，如果间接支持可以算作实际贡献，那么这种解释将几

---

116 *Ibid*., para. 39; Daniel Statman, “Targeted Killing”, *Theoretical Inquiries in Law*, Vol. 5, No. 1, 2004, pp. 179, 195.
117 本文作者在这里尽量不使用“物体”一词，因为关于是否存在非人类目标也非“物体”的问题将在下文中讨论。
118 《第一附加议定书》第 52 条第 1 款；《红十字国际委员会习惯法研究》，前注 12，规则 9，第 31～32 页。
119 《第一附加议定书》第 52 条第 2 款；《红十字国际委员会习惯法研究》，前注 12，规则 7，第 24～28 页。
120 《第一附加议定书》第 52 条第 2 款；《红十字国际委员会习惯法研究》，前注 12，规则 8，第 28～31 页；Jacob Kellenberger, “International Humanitarian Law at the Beginning of the 21st Century”, statement given at the 26th Round Table on Current Problems in International Humanitarian Law, Sanremo, 5–7 September 2002.
121 DoD, above note 41, p. 210; Charles J. Dunlap, “The End of Innocence: Rethinking Non-Combatancy in the Post-Kosovo Era”, *Strategic Review*, Vol. 9, 2000, p. 17; US Department of the Navy and Department of Homeland Security, *The Commander’s Handbook on the Law of Naval Operations*, July 2007, para. 8.2. 也有一些相反的观点，如 Laurent Gisel, “The Relevance of Revenue-Generating Objects in Relation to The Notion of Military Objective”, in ICRC, *The Additional Protocols at 40: Achievements and Challenges*, 18th Bruges Colloquium, 19–20 October 2017。
122 Program on Humanitarian Policy and Conflict Research at Harvard University, *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, MA, 2010, p. 49.
123 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on APs), para. 2018.
124 E. Mavropoulou, above note 51, p. 44.
125 Marco Sassòli, “Military Objectives”, in *Max Planck Encyclopedia of Public International Law*, 2015, para. 7.
126 J. Kelsey, above note 33, p. 1440.

乎是毫无限制的，因为它将使“任何影响到敌方作战能力的信息功能都有资格成为合法目标”。[127]因此，这种宽泛解释不符合《第一附加议定书》第 52 条第 2 款所涉及的目的和宗旨。

所以，军事目标的定义应包含两个同等重要的要素：实际贡献和明确利益。满足前一个要素并不自动导致后一个要素的满足，因为这两个要素是独立的。在起草《第一附加议定书》时，明确利益的要素被进行了详细的讨论。被考虑和拒绝的形容词包括“明确的”“直接的”“清楚的”“即时的”“明显的”“具体的”和“实质的”。[128]很明显，“明确”这个词有它自己的价值，不应该被忽视——利益必须是明确和实实在在的。[129]潜在的和不确定形式的利益是不可接受的；政治利益也不行。[130]换句话说，发动只提供潜在或不确定利益的攻击是被禁止的。[131]

实际贡献和明确的军事利益这两个要素也是同等重要的。通常很难确定某一攻击所预期的军事利益，特别是在网络环境下，衡量网络行动的效果可能具有挑战性。[132]在网络领域，军方使用与平民人口相同的网络基础设施服务其军事活动的情况下，定义的第二个要求变得更加宽泛，人们应该对严重低估第二个要素重要性的笼统结论谨慎对待。[133]与其他目标相比，网络空间具有相对的弹性。在对通信网络等网络基础设施的攻击中，数据流非常灵活，即使某些通信路径被网络攻击破坏，数据包仍可沿各种其他可能的路径到达预定的目的地。[134]在这种情况下，部分摧毁网络可能对军事行动有实际贡献，但最终很难提供明确的军事利益。因此，对明确的军事利益的判断是复杂的，不能认为一旦实际贡献要素得到满足，就会自动提供明确的军事利益。

在网络背景下，明确的军事利益总是很难衡量和量化，如果不是完全不可能的话。在震网病毒事件发生后，尽管伊朗否认该事件造成了重大破坏，但国际原子能机构报告称，伊朗已停止向纳坦兹的数千台离心机输送铀。没有人知道震网病毒对伊朗核方案造成了什么后果，也不清楚停止使用纳坦兹离心机的决定是由于震网病毒还是由于设备固有的技术故障。[135]

在网络空间背景下特别值得一提的是，确定与攻击特定目标有关的明确军事利益的要求往往涉及潜在的军民两用物体。一个设施既可以完全用于民用目的，也可以完全用于军事目的，但它也可以同时用于这两种目的，使它成为军民两用物体。[136]诸如桥梁、发电设施和炼油设施等基本基础设施也可能同时为民用和军事目的服务。[137]

网络战的根本区别在于网络空间的独特性质，即“民用和军事基础设施的系统性互联互通”。[138]例如，据估计大约 98%的美国政府通信[139]使用平民所有和平民运营的网络。[140]民用卫星、路由器、电缆、服务器甚至计算机都是潜在的两用网络设施。现实情况是，“网络基础设施的每一个组成部分，每一点内存容量都具有军事潜力”，这模糊了民用物体和军事目标之间的界限。[141]中国空军工程大学朱莉欣教授指出，美国军队重视建设以人工智能和量子计算为支撑的弹性情报、侦察与监视（ISR）体系，积极采购智能小直径炸弹、蜂群无人系统、高超声速及定向能等武器来确保杀伤力。这个所谓的 ISR 体系需要量子计算机、卫星、人工智能等机器设备，这些设备很多都同时用于军用

---

[127] M. Roscini, above note 65, p. 186.
[128] 相应的英语和法语单词为：“distinct”（*distinct*）、“direct”（*direct*）、“clear”（*net*）、“immediate”（*immediat*）、“obvious”（*evident*）、“specific”（*specifique*）和“substantial”（*substantiel*），见 ICRC Commentary on APS, above note 123, para. 2019。
[129] Robert Kolb and Richard Hyde, *An Introduction to the International Law of Armed Conflicts*, Hart Publishing, Oxford, 2008, pp. 60, 131.
[130] ICRC Commentary on APs, above note 123, para. 2024.
[131] *Ibid*., paras 2024–2025.
[132] M. Roscini, above note 65, p. 188.
[133] R. Geiss and H. Lahmann, above note 34, p. 388.
[134] *Ibid*.
[135] Marco Roscini, “Military Objectives in Cyber Warfare”, in Mariarosaria Taddeo and Luciano Floridi (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence of Excellence Initiative*, Springer, Cham, 2017, p. 108; Katharina Ziolkowski, *Stuxnet–Legal Considerations*, CCD COE, Tallinn, 2012, p. 5, available at: https://ccdcoe.org/uploads/2018/10/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.
[136] Dominik Steiger, “Civilian Objects”, in *Max Planck Encyclopedia of Public International Law*, 2011, para. 12.
[137] *Ibid*.
[138] R. Geiss and H. Lahmann, above note 34, p. 385.
[139] 为了避免歧义，就所提到的数字而言，我们要提醒读者，并非所有的政府通讯都等同于军事通讯或军事目标。
[140] Eric Talbot Jensen, “Cyber Warfare and Precautions against the Effects of Attacks”, *Texas Law Review*, Vol. 88, No. 7, 2010, pp. 1522, 1542.
[141] R. Geiss and H. Lahmann, above note 34, p. 388.

和民用目的。[142]尽管存在这些挑战，但对法律而言，军民两用物体并不是一个单独的类别；它们必须满足《第一附加议定书》第 52 条第 2 款的双重要求。认为互联网本身可以构成军事目标的想法可能是站不住脚的，因为通过互联网使用军事代码可能会作出一些军事贡献，但它们很难说是实际的，而且它也不能证明攻击是正当的，因为仅仅中断其操作将极不可能提供必需的“明确的军事利益”。[143]在任何情况下，对整个互联网的攻击都违反了比例原则，[144]因此绝不是合法的。

此外，由于军民两用物体的概念不是网络战的创新，《第一附加议定书》在成文法上提供了一个非凡的推定：如果对物体的军事地位有怀疑时，应推定为未被这样利用。[145]《塔林手册 2.0 版》的规则 102 还规定“对通常用于民用目的的物体和相关网络基础设施是否对军事行动做出实际贡献的问题存疑的，只有经过审慎评估后才能作出其被这样利用的判断”。[146]

数据是否属于军事目标的范围

在许多社会中数据已经成为生活的基石。武装冲突期间，操纵数据造成人身伤害无疑需要国际人道法的约束，但关于数据本身是否可能构成军事目标的问题也争议重重。网络攻击能够直接针对数据，而不会造成物理影响，比如针对民用金融系统的攻击。有一些观点认为，只有物质的、有形的东西才能成为军事目标，才有资格成为合法的攻击目标。[147]在《塔林手册 2.0 版》中，只有少数专家认为某些数据应被视为物体，从而构成军事目标。[148]阐明“军事目标”一词与“物体”一词之间的关系是重要的。简而言之，从《第一附加议定书》第 52 条第 2 款的措辞来看——“就物体而言，军事目标只限于……的物体”——军事目标是指符合特定标准的物体。这里的争议点在于数据本身是否可以构成物体。质疑数据能否构成军事目标的主要理由有两个，而这两个理由都与“物体”的概念有关。第一，数据的无形属性不符合“物体”的通常意义。第二，红十字国际委员会关于附加议定书的评注指出，“一个物体被描述……为可视且有形的某样东西”。[149]因此，数据显然不符合条件。一些学者认为，数据应该被视为物体。[150]他们的论点是针对民用数据的网络行动，在事实层面上是对民用物体的非法攻击。在这些学者看来，有必要强调的是，在针对合法网络目标的行动中，对民用数据的任何直接或间接影响都必须根据比例分析原则进行衡量，并遵循将民用附带损害最小化的要求。[151]这种解释的优点是，它保护平民人口免受网络行动的潜在负面影响，但它涵盖太宽，太广泛，甚至包括一些国家已经在定期实践的网络行动，如心理行动。[152]概言之，这些对《塔林手册 2.0 版》中大多数专家所持立场的批评和质疑，集中在将数据排除在《第一附加议定书》的目标法所提供的保护之外。根据这种观点，即使没有物理后果的网络行动，只要涉及到数据的损害或破坏，即使它们可能只对平民人口产生潜在影响，也至少应该接受比例原则和预防措施原则[153]的

---

142 朱莉欣，《平战结合与网络空间国际规则制定》，前注 2，第 40 页。

143 International Criminal Tribunal for the former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia*, 13 June 2000, para. 75.

144 《第一附加议定书》第 51 条第 5 款第 2 项，第 57 条第 2 款第 1 项第 3 目。

145 同上注，第 52 条第 3 款。

146 《塔林手册 2.0 版》，前注 31，第 435 页。

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

148 《塔林手册 2.0 版》，前注 31，规则 100，第 426 页；M. N. Schmitt, above note 30, p. 269; 迈克尔·施密特，《重新布线的战争：有关网络攻击之法律的再思考》，第 96 卷，第 893 期，2015 年，第 13 页。

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

150 See, for example, Kubo Mačák, “Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law”, *Israel Law Review*, Vol. 48, No. 1, 2015; 《红十字国际委员会网络行动文件》，前注 32，第 8～9 页；《红十字国际委员会 2015 年挑战报告》，前注 32，第 39～40 页；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：〈日内瓦公约〉70 周年之际重申承诺，致力于继续在武装冲突中提供保护》，日内瓦，2019 年（《红十字国际委员会 2019 年挑战报告》），第 28 页。

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

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

153 Y. Dinstein, above note 46, pp. 164–174，指出预防措施原则包括攻击中的主动预防（《第一附加议定书》第 57 条）和被动预防（《第一附加议定书》第 58 条）。攻击中主动预防要求：“1. 尽可能查明将予攻击的目标是合法的；2. 在选择攻击手段和方法时，采取一切可能的预防措施，以期避免，并无论如何，减少平民生命附带受损失、平民受

检验。[154]其他学者不同意这种观点并认为，一旦数据符合标准，就应该将其视为军事目标。对这些学者来说，将数据解释为物体将“大大扩大战争中允许的目标类别”，[155]并与在武装冲突局势中加强保护平民的宗旨和目的背道而驰。此外，对“物体”通常意义的理解是有争议的。《第一附加议定书》的六种作准本文的翻译上存在差异。[156]法语和西班牙语的“*un bien*”一词翻译成英文可以表示“一件货物”或“一项财产”，但在法语中这个法律术语可以包括有形财产和无形财产。[157]事实上，在中文语境中，“物体”一词，[158]通常指的是“由物质构成的，占有一定空间的个体”，[159]所以无形的数据会被排除在外。

也有学者认为数据应该分为两类：“操作层面”的数据和“内容层面”的数据。[160]根据这种观点，“内容层面”的数据，例如本文的文本或医疗数据库、图书馆目录等内容，基本上不属于军事目标的范围。[161]“操作层面”的数据，即赋予硬件功能和执行任务所需能力的数据类型，将被视为军事目标。[162]

遗憾的是，民用数据是否应被视为民用物体并因此受到国际人道法保护的问题似乎没有得到中国学者的重视。国防大学政治学院朱雁新副教授认为，数据可在不构成物体的情况下被定义为军事目标。[163]他主张数据是一种“非物体”的军事目标。[164]该观点是建立在《第一附加议定书》第 52 条第 2 款开头措辞的基础上：

> 攻击应严格限于军事目标。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。[165]

这一条款的字面措辞清楚地允许物体或者非物体的军事目标的存在。

本文作者在此问题上的观点与红十字国际委员会 2019 年的立场文件基本一致。[166]某些数据，至少基本的民用数据，[167]应属于民用物体的范畴，因为“物体”一词的通常意义正在演进中，并且（这样理解）将符合日内瓦四公约及其附加议定书的目的和宗旨。“物体”一词不一定将数据排除在军事目标范畴之外；我们必须牢记，“物体”的通常意义不应局限于条约通过时的含义，而是将随着时间的推移而演进。[168]完全基于文本方法的条约解释忽略了《维也纳条约法公约》所载的其他解释方法。[169]例如，从《第一附加议定书》的目的和宗旨来看，“在这个高度依赖数据的时代，国际人道法不禁止删除或篡改……重要民用数据”的观点“似乎难以与国际人道法的目的和宗旨相一

伤害和民用物体受损害”。被动预防要求交战各方，“在最大可能范围内’，一、努力将其控制下的平民居民、平民个人和民用物体迁离军事目标的附近地方；二、避免将军事目标设在人口稠密区内或其附近；以及三、保护在其控制下的平民居民、平民个人和民用物体不受军事行动所造成的危害。

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

[155] K. Mačák, above note 150.

[156] 《第一附加议定书》第 102 条：“本议定书原本，其阿拉伯文、中文、英文、法文、俄文和西班牙文各本同样作准……”。

[157] K. Mačák, above note 150.

[158] 中文版的《第一附加议定书》使用的是“物体”一词。见 www.icrc.org/zh/doc/assets/files/other/mt_070116_prot1_c.pdf。

[159] “由物质构成的，占有一定空间的个体”。见《当代汉语词典》，上海辞书出版社 2001 年版；《现代汉语大词典》（下册），上海辞书出版社 2009 年版；《新华汉语词典》，崇文书局 2006 年版；《近现代词源》，上海辞书出版社 2010 年版。

[160] Heather Harrison Dinniss, “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives”, *Israel Law Review*, Vol. 48, No. 1, 2015, p. 41.

[161] *Ibid*.

[162] *Ibid*.

[163] 朱雁新：《数据的性质：对军事目标法律含义的重新解读》，载黄志雄主编：《网络空间国际规则新动向：〈塔林手册 2.0 版〉研究文集》，第 410～413 页。

[164] 同上注，第 410 页。

[165] 《第一附加议定书》第 52 条第 2 款。

[166] 《红十字国际委员会网络行动文件》，前注 32，第 7～8 页。

[167] 同上注。

[168] K. Mačák, above note 150.

[169] 见《维也纳条约法公约》，1155 UNTS 331，1969 年 5 月 23 日（1980 年 1 月 27 日生效），第 31 条第 3 款甲项。

致”。[170]一个令人信服的论点是，用数据形式的数字文件取代纸质文件和资料不应减少国际人道法为其提供的保护。[171]如果数据不是物体，针对民用数据的网络行动就会成为国际人道法的真空，且对平民生活造成重大损害的网络行动并不受法律禁止。[172]

《塔林手册 2.0 版》将军事目标与物体等同起来。为了说明这一点，规则 100 中所提出的军事目标的定义没有给非物体留下余地：“军事目标是……的物体”。[173]认为数据可以构成非物体的军事目标的观点是值得怀疑的，原因有二。首先，这一观点将动摇传统的人/物二分法，就这些规则的建构而言，这种二分法似乎是正确的；各国甚至拒绝了第三种类别，如“地点”。[174]其次，这样一来就没有有效的标准来评估某一特定数据集是否构成军事目标。[175]人/物二分法为非生物提供了实际贡献和明确利益的双重标准，而对生物目标则有其他要求。[176]如果数据不属于物体，这将导致一个不合理的立场，即数据需要在与生物目标（即人类）相同的基础上进行评估。因此，将数据定义为非物体的军事目标的观点不具有说服力。

结论

西塞罗的格言“在战争中，法律寂静无声”（*silent enim legis inter arma*）并不反映当代现实。尽管存在种种挑战，但战时法中的区分原则适用于网络战。由于缺乏专门针对网络领域的条约规定和司法裁决，对既有法律的解释基于现有的学术讨论和有限的国家实践。有必要对网络背景下的区分原则进行普遍澄清和进一步发展；例如，“网络军事目标”和“网络战斗员”的定义仍存在争议。诚如联合国秘书长在世界经济论坛上所提到的那样，“我们需要在如何将这些新技术融入几十年前在完全不同的背景下定义的战争法的问题上，在世界范围内达成最低限度的共识”。[177]

截至目前，中国政府对国际人道法在网络空间的适用（的立场）尚不明确。中国确实有研究国际人道法适用于网络空间的学术论文，但对网络空间区分原则的讨论在篇幅和学术深度上都很有限。与西方相比，中国学者对这一问题的研究还处于比较初级的阶段。目前，中国学界还没有对区分原则之于网络空间的适用进行具体的解构或澄清。

尽管存在潜在的技术挑战和不确定性，但区分原则应适用于网络空间。区分原则之于网络空间的适用还应从防止过度军事化和最大限度地保护平民利益的立场上仔细重新审视和澄清。就人类目标而言，习惯国际法和相关国际人道法条约中确定谁是战斗员的要素不太适合数字战场。然而，网络战斗员仍然有义务将自己与平民区分开来。在适用区分原则时，本文作者认为，关注实质要素比关注形式要素更有意义，例如公开携带武器或备有可从远处识别之固定的特殊标志。在解释“直接参加敌对行动”时，损害下限要求有客观可能性而不仅仅是主观意图，且应确认交战联系，而因果关系的确认至少应满足近因的要求。类比运用“网络杀伤链”模型，有助于我们把握网络战中直接参加敌对行动的全过程。对于非人类目标，所有军事目标都必须同时满足实际贡献标准和明确的军事利益标准，二者缺一不可。同样的要求也适用于军民两用物体。至于数据的地位，“物体”的通常含义是有争议的。《第一附加议定书》的六种作准文本存在翻译差异。在法语中，这一法律术语既包括有形财产也包括无形财产；而在中文中，这一术语一般是指那些由材料构成的占有一定空间的物品，因此无形数据不计算在内。此外，一位中国学者认为，某些数据属于“非物体”的军事目标范畴。

随着互联网技术的普及，二十一世纪发生了前所未有的变化。国际人道法在网络空间的未来仍掌握在各国手中，特别是在各国解释现有规则和规范时。自有组织的人类冲突开始以来，战争、技术和战时法在实质性地相互交织，相互影响，但法律一直被迫不断调整，似乎总是“落后于一场战

[170] 《红十字国际委员会网络行动文件》，前注 32，第 8 页。
[171] 《红十字国际委员会 2019 年挑战报告》，前注 150，第 28 页。
[172] See M. N. Schmitt, above note 151.
[173] 《塔林手册 2.0 版》，前注 31，第 424 页。
[174] M. Bothe, K. J. Partsch and W. A. Solf, above note 87, pp. 301–304.
[175] K. Mačák, above note 150.
[176] 《第一附加议定书》第 52 条第 2 款。
[177] World Economic Forum, ‘António Guterres: Read the UN Secretary-General’s Davos Speech in Full’, 24 January 2019, available at: www.weforum.org/agenda/2019/01/these-are-the-global-priorities-and-risks-for-the-future-according-to-antonio-guterres/.

争”。[178]因此，面对技术和科学的变化，最好是使用对国际条约和国际法原则进行动态和演进解释的方法，以便使它们充分发挥作用。必须认识到，武器的日益发展及科学和技术的迅速发展将对人类社会产生巨大的影响，战时法将作出相应的调整和适应。然而，如果认为国际人道法的改变将会既及时又有效，那就太天真了。

现在提倡在该领域通过一项新条约可能还为时过早。无论如何，各国在不久的将来就一项关于网络战的全面公约达成一致的前景是相当渺茫的。取而代之的是，现有的实然法提供了网络领域针对目标的基本规则。国家实践、司法判决以及学者观点和学说应率先对现有法律框架进行解释，并评估其所服务的人道主义关切在互联互通的网络空间领域中是否得到满足或遭到破坏。可以预见的是，在这一演变过程中，各国在网络战时代实施新战略时，可能试图类比推理、诱导或创造性地填补现有国际人道法的空白，或推动有关区分原则的实然法超越其规范边界。这种趋势需要受到严格限制；但是，排除制定新规则的可能性是武断的。从防止过度军事化和最大限度保护平民利益的角度出发，有必要慎重再解读这一原则。虽然到目前为止还没有发生大规模伤亡的网络事件，但当对现有规则的解释和澄清还不够时，需在“网络珍珠港”事件发生之前提出新的规则。[179]

[178] Jimena M. Conde Jiminián, “The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law”, *Tilburg Law Review*, Vol. 15, No. 1, 2010. See also Marco Sassòli, Antoine Bouvier and Anne Quintin, *How Does Law Protect in War?*, 3rd ed., Vol. 1, ICRC, Geneva, 2011, p. 52.
[179] DoD, above note 4; J. J. Wirtz, “The Cyber Pearl Harbor”, above note 4; J. J. Wirtz, “The Cyber Pearl Harbor Redux”, above note 4.