论军民融合趋势下网络武装冲突适用区分原则

焦园博*

摘　要：随着各国网络空间军事化进程加快，网络武装冲突适用区分原则面临军民融合趋势的挑战。军民融合在性质上混同了军用与民用属性，进而易引发不分皂白的网络攻击。基于此，国际社会若在网络空间中适用区分原则，就要分析其中的利益平衡。当前在军事需求与人道主义保护之间，应当更加重视人道主义保护。在审视区分原则的适用性方面，对军事目标“可攻击性”涉及的“实际贡献”与“军事利益”应作出严格解释，强调“现实性”与“不可替代性”，并强化攻击行为的“可控制性”。国际社会对于网络空间中适用区分原则的立场应当是强调人道主义保护属性，强化《联合国宪章》的地位，遏制网络武装冲突合法化的趋势，通过鼓励合理军民分离来实现人道主义保护诉求。

关键词：网络武装冲突　区分原则　国际人道法　军民融合　塔林手册

随着互联网技术的爆炸式发展，制网权成为世界权力图谱的新的关键要素，各国对于军用、民用网络技术的重视已达到前所未有的程度。“世界各大国均把信息化作为国家战略重点和优先发展方向，围绕网络空间发展主导权、制网权的争夺日趋激烈，世界权力图谱因信息化而被重新绘制，互联网成为影响世界的重要力量。”①

虽然最早的网络技术由军用技术推广而来，② 但许多国家已从 20 世纪 90 年代以来的民用网络技术更迭中发现民用技术的强大潜力，通过施行军民融合政策，希望民间技术成为巩固“网络边防”的重要力量。在这个过程中不容忽视的问题是，军用网络技术的发展将可能加剧全球网络空间的紧张态势、引发网络空间武装冲突。即使如今还没有真正意义上的网络战出现，但一些网络行为无疑隐含着战争风险。在此背景下，解释网络空间中适用国际人道法③的相关规则时，区分原则及其适用问题应当受到重视。区分原则在网络武装冲突中的正确适用对于军民融合趋势的长远发展具有重要意义。

---

* 焦园博，国防科技大学军政基础教育学院，讲师。本文系国家社会科学基金项目“外空活动中网络攻击行为的国际法规制研究”（2022 – SKJJ – C – 079）和国防科技大学科研计划项目“网络空间作战适用国际法的规则议定权研究”（JS21 – 3）的阶段性成果。如无特别说明，本文网络文献的最后访问时间统一为 2023 年 5 月 26 日。

① 中共中央党史和文献研究院：《习近平关于网络强国论述摘编》，中央文献出版社 2021 年版，第 41 页。

② 阿帕网（ARPANET）为美国国防部高级研究计划署开发的世界上第一个运营的封包交换网络，是全球互联网的前身。

③ 国际人道法也称为武装冲突法、战时法。本文使用国际人道法的概念表述，但对于引文中出现的武装冲突法未作改动。

一　军民融合趋势下的网络武装冲突

第二次世界大战后，世界各国将重点转移到经济建设上，并采取以经济和科技竞争为主、军事力量竞争为辅的战略，促进了军民共用技术的巨大发展，形成了各自的军民融合发展模式。[①] 从追求国家发展的角度来说，军民融合政策效果显著，因此长期以来一直作为各国的主流国家战略而存在，至今仍然意义重大。

（一）军民融合趋势的新领域：网络空间军民融合

军民融合政策自提出以来，在各国表现出多种形式。例如，美国的军民融合政策就历经 3 个不同阶段，俄罗斯、日本以及欧盟一些国家也采取了适应各自国情的军民融合政策。[②] 总体来看，军民融合政策旨在将国防和军队建设融于社会经济发展体系之中，为彼此提供一种可持续发展的路径。这一路径对于网络领域发展而言同样不可忽视。

自 20 世纪 90 年代以来，在网络空间施行军民融合政策逐渐受到各国重视。网络空间的军民融合政策在客观上是军用、民用两个领域技术发展侧重方向不同所致。国家既希望民用技术从军事领域得到进一步的技术启发，同时也希望将民用技术融入军事活动中，在国家网络安全方面提供技术创新、设施共建、信息共享、作战支撑等方面的助力，由此形成一种较为典型的“军民一体化”[③] 模式。目前网络空间的技术发展尚未看到尽头，想要在网络空间安全方面取得长久成效，需要依托军民融合路径。

在传统军民融合领域，如航空航天业、军工制造业等领域，军民融合更多地体现为军事技术与民间资源的整合。然而，在互联网领域，军民融合表现出不同的样态。近年来，民间网络技术及资源的发展程度突飞猛进，因此对于网络空间军民融合而言，反而更多表现为民间技术及资源的“反哺”。网络空间军民融合在军事层面的目标，不仅在于推进国防信息技术创新，还表现在军地共建国家信息基础设施、军地共享网络威胁信息资源以及构建军地作战联合协作机制等方面。在军地共建国家信息基础设施方面，大多数军用网络事实上依靠民用（主要是商业）计算机基础设施，如海底光纤电缆、卫星、路由器或节点；而民用车辆、航运和空中管制系统配备军用的基于全球定位卫星导航系统的情况也越来越普遍。[④] 据报道，美国政府约 98% 的信息是通过平民所有或经营的网络传递。[⑤] 在军地共享网络威胁信息资源方面，以美国为例，美国鼓励私有部门与政府、军队实时共享网络安全威胁信息，这将有效提高情报研究分析的专业性，促进网络安全威胁信息的利用和实时响应能力的提升。[⑥] 在军地作战联合协作机制方面，例如美国构建了

---

① 牛振喜：《各国军民融合的历程及我国军民融合的对策》，载《科技进步与对策》2011 年第 23 期，第 124 页。

② 叶选挺、刘云：《美国推动军民融合的发展模式及对我国的启示》，载《国防技术基础》2007 年第 4 期，第 41—42 页。

③ 较为典型的融合模式有“军民一体化”“以民掩军”“先军后民”“以军带民”4 种模式。参见杜人淮：《国外推进国防工业军民融合发展的借鉴与启示》，载《南京政治学院学报》2010 年第 5 期，第 37 页。

④ Cordula Droege, “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians”, (2012) 94 *International Review of Red Cross* 533, p. 539.

⑤ Eric Talbot Jensen, “Cyber Warfare and Precaution Against the Effects of Attacks”, (2010) 88 *Texas Law Review* 1533, p. 1534.

⑥ 刘彬、胡建伟、康绯：《美国网络空间军民一体化组织运行体制及启示》，载《网信军民融合》2019 年第 2 期，第 58 页。

由传统国家安全部门牵头，融合应急事件报告机构、网络服务提供商、私营软件开发商等私营机构展开作战配合的协同体系，通过军民联合攻防演练机制、“网络靶场”等项目集合民间力量，提升军民一体的网络攻防水平。[①] 可以看到，在上述各方面的融合中，国家都在试图将民用要素作为作战力量纳入作战体系。

（二）军民融合趋势下的网络武装冲突态势

军民融合为一国的军事活动带来各类优势，此种优势既可能应用于防御性军事活动，也可能应用于进攻性军事活动。在国家间网络对抗日益紧张的今天，国际社会面临着一些国家通过军民融合措施追求进攻性作战能力的巨大风险。

当前国家层面的网络对抗活动已不再少见。自互联网普及以来，互联网因素在国家对抗中的存在感日益提升，如2010年被发现的美国对伊朗核设施采取的“震网”（stuxnet）病毒攻击，2016年美国对“伊斯兰国”恐怖组织实施的“网络战”，2020年俄罗斯与美国之间发生的“太阳风”（solar winds）网络攻击事件。而在传统的武装冲突场合，互联网的影响也日益可见。以上事件都在一定程度上折射出国家主体寻求将网络因素作为对抗手段。国家间的网络活动显然有别于一般网络攻击，其关键区别在于国家意志的体现与否。当国家主体出现在攻击性网络活动中时，网络活动的性质将迥然不同，其规制方式也全然不同。[②]

从现有的理解来看，网络武装冲突更多表现为传统物理性武装冲突所伴随的网络攻击行为，但较多依附于传统物理性冲突（physical conflict），并不代表仅仅基于网络条件的武装冲突不存在。从未来网络安全价值的发展趋势来看，独立存在的网络攻击涉及“敌对行为”时，其危害性完全有可能达到物理性冲突的程度，其必不能为《联合国宪章》彰显的国际法治所容忍。因此，仅基于网络方式的攻击也应当被界定为国际人道法意义上的“敌对行动”。如今学界研究以更为精准的“网络武装冲突”（cyber armed conflict）[③] 概念指代上述网络领域的军事化行动，这也将是本文所采取的表述方式。网络武装冲突的通常含义要求存在“敌对行动”，这意味着作战手段和方法的运用，[④] 更确切地说是使用了导致“攻击”（attack）[⑤] 后果的作战手段和方法，无需与传统物理性冲突相结合，且有别于通常所使用的“网络攻击”概念。[⑥]

国际社会目前在规制网络武装冲突方面达成的共识较为有限，网络武装冲突本身已是国际社

---

① 刘彬、胡建伟、康绯：《美国网络空间军民一体化组织运行体制及启示》，载《网信军民融合》2019年第2期，第57—58页。

② 一般网络攻击在性质上更多由国内法加以规制，依据其严重程度可能体现在民法、行政法、刑法各个层次，并可能经由国际刑事司法合作实现国际层面的规制；国家参与的攻击性网络活动是国家意志的延伸，具有突出的军事化特点，可能受国际法规则的规制，武装冲突法、国家责任法等都可能成为该领域的法律渊源。

③ 参见蔡高强、焦园博：《“网络武装冲突”的国际法阐释》，载《湘潭大学学报（哲学社会科学版）》2017年第3期，第16—23页。

④ 〔美〕迈克尔·施密特等：《网络行动国际法塔林手册2.0版》，黄志雄译，社会科学文献出版社2017年版，第378页。

⑤ 本文认为，“攻击”指针对敌方使用暴力行为，对暴力的理解不局限于使用物理性武力的行为，非物理性网络攻击也可能构成暴力。通常对攻击的理解应包含损害因素，更重要的是从攻击后果层面认定攻击的存在。网络层面的攻击一定程度上具有便捷的可恢复性，因此涉及网络攻击损害的界定更加特殊，应当认为程度上达到需作出物理层面的补救时构成攻击。从这个意义上说，2010年“震网”病毒事件无疑属于攻击范畴。

⑥ “网络攻击”是更为具体的行为范畴，其可能存在于网络武装冲突中，也可能存在于网络犯罪中，网络武装冲突意义下的网络攻击更宜结合武装冲突法中关于攻击的界定来讨论。

会面临的难题，当这一问题关涉“军民融合”政策时，将带来更为复杂的局面。军民融合政策在国家层面可以增进国防和军事水平的进步，但却在国际法层面带来新的法律问题。进入信息化时代，战争进程正大幅度缩短，平时与战时的界限也越来越模糊。[①] 在军民融合趋势下，此种模糊性愈加难以分辨。从网络武装冲突的角度来说，由于民用网络基础设施路径被用于传递军事情报，因此属于军事目标，对其予以打击几乎总是被认为是正当的。[②] 在爱沙尼亚、格鲁吉亚曾遭受的网络攻击中，就因无差别的攻击致使大范围网络设施瘫痪（包括政府网站、民用网站等）。从攻击者的视角看来，任何网络节点都可能被用于实施反击。军民融合措施更是强化了此种能力，因此攻击者更倾向于在实施网络攻击时不留任何余地，致使网络攻击对民生造成重大影响，国际人道法中的区分原则被彻底忽视了。

可以看出，军民融合趋势在网络武装冲突领域带来的问题在于，军民融合政策将导致区分原则更加难以适用。由此产生的挑战是，在潜在的网络武装冲突中，军民融合政策与区分原则之间是否可以实现有效调和，以确保国际法人道主义保护目标的实现。

二　传统原则与全新情势：区分原则与军民融合政策的碰撞

如恩格斯所言：“一旦技术上的进步可以用于军事目的并且已经用于军事目的，它们便立刻几乎强制地，而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革。”[③] 当前主要的网络技术大国都在强化将网络技术应用于作战的能力，军民融合正是各国综合运用社会力量来提升网络空间作战能力和网络空间安全防护能力的关键策略。越是在此种趋势之下，国际社会越需要关心国际法人道主义保护目标的实现。

（一）区分原则在网络武装冲突中的适用前景

关于国际人道法是否可在网络空间中适用，一类立场主张当前不宜讨论此问题，理由是避免变相承认网络武装冲突的合法性。虽然此观点确有其合理性，但是应当看到，军民融合政策的目标已确实指向网络空间的军备竞争，为网络空间的稳定性带来挑战，其中潜在的国际人道问题已难以被回避。面对网络空间的新军备竞赛，其解决方案应当是将已有国际人道法在网络空间的适用严格限制于人道主义保护的目的。这一点在《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》中得到强调：需要进一步研究这些原则（人道原则、必要性原则、相称性原则和区分原则）如何以及何时适用于各国对信通技术的利用，并强调回顾这些原则绝不是要给冲突披上合法外衣或鼓励冲突。[④] 其中，区分原则由国际法院在“威胁使用或使用核武器的合

① 张孟麒、陈刚、张纪元：《军民融合网络空间作战指挥体系构建研探》，载中国指挥与控制学会：《第九届中国指挥控制大会论文集》，2021 年，第 102 页。

② Cordula Droege, “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians”, (2012) 94 *International Review of Red Cross* 533, p. 564.

③ 〔德〕弗里德里希·恩格斯：《反杜林论》，载《马克思恩格斯全集（第 20 卷）》，中共中央编译局译，人民出版社 1971 年版，第 187 页。

④ 联合国大会：《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 7 月 14 日，第 71（f）段。

法性案”（*Legality of the Threat or Use of Nuclear Weapons*）咨询意见中确认为国际人道法的两个首要原则之一，[①] 被认为是不可减损的，也是本文所关注的重点。

在论证区分原则在网络武装冲突中的可适用性的过程中，主要的支持观点体现为《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》（以下简称《日内瓦公约第一附加议定书》）、国际法院的咨询意见以及联合国专家组共识性文件的相关条文中。其一，《日内瓦公约第一附加议定书》所述及的审慎义务[②]及马顿斯条款（Martens clause）[③] 对于论证区分原则在网络空间武装冲突中的可适用性方面效果有限。由于区分原则本身出自《日内瓦公约第一附加议定书》，通过引用《日内瓦公约第一附加议定书》相关条款来证明此种可适用性属于对文本的自我解释，缺乏外部合理性论证。其二，国际法院在“威胁使用或使用核武器的合法性案”中指出，国际人道法的既定原则和规则适用于任何形式的战争和武器。[④] 由于国际法院咨询意见并无约束力，因此以上材料并不直接证成国家间的新合意。其三，2015 年联合国信息安全政府间专家组报告述及：“专家组提到的既定国际法律原则，包括适用情况下的人道原则、必要性原则、相称原则和区分原则。”[⑤] 其言下之意为：此 4 项原则目前并非已被认可适用于当前的网络空间议题，但当存在相应的武装冲突情境时，无疑应当予以考虑。联合国大会文件虽无拘束力，但在集中表达国家间合意方面极具意义。此外，诸如《网络行动国际法塔林手册 2.0 版》（以下简称《塔林手册 2.0》）等非官方文本则直接确认了区分原则等国际人道法原则的适用。[⑥] 以上 3 类文件中，联合国专家组的共识性文件在增进区分原则的适用方面最具价值。从趋势上看，在网络武装冲突中适用区分原则是不可回避的议题，提早展开对区分原则适用方式的讨论是必要的。

对于区分原则在网络武装冲突的实际适用，一些观点从理论分析层面表现出悲观态度。网络空间自诞生以来便存在军民两用目标，但军民融合趋势的发展使此种目标泛化，导致对于此类目标的属性更难界定、保护更难实施。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。[⑦] 更有观点直接指出，区分原则在网络空间中似乎不大可能起到保护民用网络基础设施以及所有依靠网络的民用基础设施的作用。[⑧] 以上观点将军民融合政策置于区分原则的对立面，没有为问题的解决提供任何助益，因此并不可取。

应当认为，网络空间的军民混用性以及增进此种性质的军民融合在客观上导致网络空间目标

---

① *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J Reports 1996, para. 78.

② 《日内瓦公约第一附加议定书》第 36 条规定：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。

③ 《日内瓦公约第一附加议定书》第 1 条第 2 款规定：即使没有条文的规定，平民和战斗员仍受来源于既定习惯、人道原则和公众良心要求的国际法原则的保护和支配。

④ *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I. C. J Reports 1996, para. 86.

⑤ 联合国大会：《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》，A/70/174，2015 年 7 月 22 日，第 28（d）段。

⑥ 《网络行动国际法塔林手册 2.0 版》第 93 条规定：区分原则适用于网络攻击。参见〔美〕迈克尔·施密特等：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 411 页。

⑦ 参见克努特·德尔曼、洛朗·吉塞勒、蒂尔曼·罗登霍伊塞尔：《国际人道法对网络战的可适用性及其适用》，丁玉琼译，载《国际法研究》2019 年第 4 期，第 13 页。

⑧ Cordula Droege, “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians”, (2012) 94 *International Review of Red Cross* 533, p. 566.

的属性混同，但不能消除国家在参与网络武装冲突时的人道主义保护义务。真正涉及军事活动的网络设备设施占比毕竟为少数，民用网络遭受攻击波及的可能性较大，当实际发生武装冲突时，民用网络将首当其冲受到攻击。此时，国际法须对此类行为予以回应，尤其需要判定有关行为是否违背区分原则，以实现区分原则所代表的正当价值。

（二）核心关切：军事需求与人道主义保护要求的平衡

在军民融合趋势下，网络作战技术的更新迭代频繁，军民融合使网络作战能力的发展更加不对等，进而使网络武装冲突爆发的可能性急剧增加，且社会整体对网络空间的依赖性越强，在网络空间实施作战的战略价值越高。其一，各国在网络作战能力建设及网络攻防策略的选择上态度不一致，直接参与网络作战的能力不对等。其二，各国在互联网的民用领域发展程度不一致，民用领域支持本国参与网络作战的能力同样不对等。当此种不对等达到一定程度，网络作战能力强国势必会寻求网络作战的合法化，这正是当前美国等国家推动的议程。从这个角度来说，确保国际人道法基本原则的适用严格限制在人道目标方面是极为必要的。区分原则在网络武装冲突中的适用应当更多偏向人道主义保护要求，而削弱军事需求的目的。

从军事需要的角度来看，网络空间军民融合从设施设备、数据信息、组织形式各个层面都融合了军用与民用目标，其目的就是借助社会力量强化自身的国家安全体系。除了特别用于军事用途的某些网络之外，要想区分纯民用和纯军用网络基础设施是非常困难的。[①] 从设施设备角度来看，网络武装冲突的潜在目标，既涉及预警侦察、防空反导、指挥网系等战场网络目标，也涉及通信基础设施、电信网、关键业务网等战略网络目标，后者则大量涉及民用网络。从数据信息角度来看，如果信息无法通过某个特定渠道传递，还有多种其他民用路径和选择，这样做的结果是在某些情况下，由于每个部分都可能用于传递军事情报，使整个互联网的几乎所有部分亦可能成为军事目标。[②] 从组织形式角度来看，在网络攻防演练中融入民间力量，将一些民用领域的企业、人员纳入网络作战的备战中，在各类网络安全服务提供商方面表现最为明显。在以上各个层面中，各国主动将部分民用网络纳入国家网络安全体系中，国家经由军民融合政策发展其军事需要的做法，更多以自身安全利益为核心。

从人道主义保护的角度来看，区分原则所蕴含的更普遍的价值诉求没有得到充分展示。其中的主要原因可能在于网络自身的特性模糊了网络目标的“可识别性”，致使区分原则的底线在网络环境中不断被挑战。国际人道法对于军事与非军事目标的区分主要见于《日内瓦公约第一附加议定书》第 36 条、第 48 条、第 51 条第 4 款、第 51 条第 5 款和第 52 条，其中对于目标属性的判定，不仅关乎区分原则的判定，还有可能涉及对于“使用武力”行为的判定。[③] 关于区分原则

---

① 参见克努特·德尔曼、洛朗·吉塞勒、蒂尔曼·罗登霍伊塞尔：《国际人道法对网络战的可适用性及其适用》，丁玉琼译，载《国际法研究》2019 年第 4 期，第 14 页。

② Cordula Droege，“Get off My Cloud：Cyber Warfare，International Humanitarian Law，and the Protection of Civilians”，（2012）94 *International Review of Red Cross* 533，p. 564.

③ 学者对于“使用武力”如何定性的观点大致可以分为 3 类：工具主义、目标主义和影响主义。第一种方法分析的是在攻击中所使用的工具类型；第二种方法关注的是攻击所意在指向的目标；而第三种方法注重的是特定行为造成的最终结果或影响，其中后两类主要观点都是结果导向。在迈克尔·施密特（Michael Schmitt）所提出的“规模和后果论”的 7 点标准中，“严重性”与“推定合法性”都存在对攻击目标属性的判定。参见徐奇、崔森、章成：《2013 年西方武装冲突法前沿研究趋势述评》，载《成都理工大学学报（社会科学版）》2015 年第 6 期，第 86 页。

的判定问题，在具体适用中存在一定困难。传统武装冲突中“可识别性”（identifiable）是一项基本规则，其有效保障战时权利义务的归属主体，且“可识别性”也被事物的客观性所保障。在网络活动中，“匿名性”（anonymous）则是基本规律，从根源上对“可识别性”形成挑战。区分原则是从被攻击者的角度来区分目标的，旨在确保被区分的非军事人员及目标不被攻击。然而以上条款中涉及的各类要素在网络武装冲突中无法得到有效展示，被攻击对象本身的“可识别性”较弱，非军事目标无法得到有效保护，由此导致的结果便是违反区分原则的情形在这种新型武装冲突中比在常规战争中还要常见。①

综上，在当前军民融合政策的发展背景下，国家行为体发展基于军事需求的个体安全的意愿更强，军事需求被居于优先的地位，致使由国际公约所维护的普遍的人道主义价值得不到有效维护。日内瓦体系中的诸公约在本质上都是追求人道主义保护目标，无论是战斗员、战俘、平民、难民，都具有作为人而享有的基本人权，保护这一基本人权则是人道主义保护的基本要求。一般而言，人道主义保护的界限在于武装冲突行动危及人类生存，因此通常不易产生物理性损害的网络武装冲突较难符合人道主义保护问题的基本前提。但是在网络攻击技术不断更新迭代的背景下，对该问题依然需要加以探讨。网络领域已成为人类社会的基本方面，其地位从附加价值转向基本价值，因而其上所附着的权利也开始转向基本人权，传统基础设施网络安全以及网络基础设施安全都直接关涉生存问题。例如对本身危险系数较高的核电站之类的关键设施的网络攻击极有可能造成大规模物理性损害，危及周边地区的人类生存。从以上角度考虑，人道主义保护必须成为未来网络武装冲突中优先追求的目的，尤其在军民融合政策背景下，区分原则的适用必要性只增不减。

对于以上问题，需要重新明确网络武装冲突中人道主义保护要求的边界，追求与军事需求目的之间的合理平衡，将当前状态更多地拉向人道主义保护目的。在一定程度上，应当允许在军民融合背景下对参战民用目标的合法攻击（如民用目标直接参与或用于作战），合理释放国家的军事需求，避免国家因无法满足需要而放弃遵守国际法。但在另一层面上，应当认识到国家在军民融合趋势下刻意寻求目标属性的混同，对区分原则的适用形成挑战。因此应当更为严格地界定区分标准，以满足区分原则背后的人道主义保护要求。区分原则本身的目标在于界定对特定目标实施攻击的合法性问题，可以通过对“可攻击性”和“可控制性”的分析来加以审视。

三　区分原则要件内涵的再理解

对于区分原则的重构命题来说，明确当前人道主义保护需要更为优先的同时，对于区分原则的具体内涵也要予以重新界定，置于军民融合背景之下进行再分析，以更为合理的方式保障区分原则可以在网络空间适当地适用。

网络作战中的区分原则更为集中地体现在对攻击目标的理解和认定上，因此“如何认定攻

① Jeffrey TG. Kelsey, “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare”, (2007 – 2008) 106 *Michigan Law Review* 1427, p. 1439.

击目标是合法的攻击目标”是问题核心所在，简言之即目标的“可攻击性”。[①]《日内瓦公约第一附加议定书》第 52 条第 2 款明确对军事目标予以界定：“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。”该条款在用语上的延展性为将其适用于网络武装冲突提供了基础。根据该条款，网络空间作为军事目标的要件可归纳为“实际贡献”（effective contribution）和“军事利益”（military advantage）。

（一）区分原则中实际贡献的再理解

从实际贡献角度来说，潜在目标和军事行动之间应有密切关系，强调目标的军事性。这种性质一般是通过 4 个标准确立的，即性质、位置、目的和用途。上述 4 个标准并非充分必要的，不具有军事性质的物体也可能因所处的特定位置、目的或当时的用途而对军事行动作出实际贡献。

一般认为，即使其军事用途与其民用目的相比微不足道，该物体仍可构成军事目标。例如，美国认为帮助作战能力（war-fighting capability）和维持战争能力（war-sustaining capability）也构成有效贡献。[②] 这就意味着，任何纳入军民融合措施的民用网络设施、节点都可能成为“合法的”（其认为合法的）攻击目标。更进一步来说，帮助作战能力可能意味着所有涉及军民融合的网络设施，乃至敌对国家的所有网络基础设施或关键节点将被认定为“合法的”攻击目标。

上述立场过分地将区分原则的边界拉向军事需求一侧。对此，应当主张合理地解释与适用区分原则。实际贡献这一要素应突出地表现为对作战贡献的“现实性”（practical），而非其性质、位置等因素所表现出对作战贡献的“可能性”（possible）。具体而言，基于军民两用目标在当时情境中所处的现实活动状态，判定其是否对军事行动存在实际贡献，进而确定其是否为合法的攻击目标。从这个意义上说，实际贡献这一标准应当被理解为“现实贡献”（practical contribution）。此种考量乃是因为“军民两用”概念本身即是从“可能性”判断目标的属性，若在实际的网络对抗中采取此种基于“可能性”的判断，客观上会导致“可能性”本身的无限扩大，乃至不加区分地将任何目标都界定为军事目标。

事实上，《塔林手册 2.0》主张：“兼具军用和民用目的的网络基础设施属于军事目标。”[③] 以上观点从二分法的角度指出一个物体要么是民用物体，要么是军事目标，[④] 不加区分地将“可能性”确定为既成事实。从武装冲突的角度来看，《日内瓦公约第一附加议定书》已经明确了

---

① 根据传统武装冲突法，区分原则同时涉及对人员因素和物质因素的区分。在网络武装冲突背景下，此处所述目标，则更多的指向物质因素，而不考虑人员因素。其原因在于：其一，从攻击者的角度来说，对人员要素的区分可能涉及“是否构成网络武装冲突”，“如何承担国际法上的责任”等问题，但由于此处探讨的是“可攻击性”，因此对攻击者的区分在本主题下缺少意义。其二，在网络环境下，攻击者发起攻击的直接攻击对象是物质因素，并不能直接针对人身发起攻击（在网络武装冲突环境下，人员因素不可察知且不可推断），因此从被攻击者的角度来看，对人员因素的区分在本主题中的讨论价值也不大，对于攻击目标属性判定才是重点所在。因此本主题的探讨将不特别涉及对人员因素区分的探讨。

② USA Department of the Navy and Department of Homeland Security, The Commander's Handbook on the Law of Naval Operations, July 2007, para. 8. 2.

③ 《网络行动国际法塔林手册 2.0 版》规则 101。参见〔美〕迈克尔·施密特等：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 433 页。

④ 《网络行动国际法塔林手册 2.0 版》规则 101 注解 1。参见〔美〕迈克尔·施密特等：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 433 页。

“民用”为“非军用”,[①] 而军用在本质上是实践性术语，其内容在“可能性”的意义上极易被扩展，任何一丝潜在的军用“可能性”都会排除目标的非军用属性。从人道主义保护的角度出发，以上趋势是极为危险的，本质上与区分原则的精神内涵相违背，因此，在实际贡献这一层面回到“现实性”是必要的。需要讨论的命题在更精准的意义上应当是“基于当时的现实状态，某目标是否为合法的攻击目标”，而非简单的“某目标是否为军事目标”。由此，军民融合措施下的通用设施可以不被直接认定为军事目标。

（二）区分原则中军事利益的再理解

从军事利益角度来说，实施攻击使潜在目标失能意味着实现了军事利益，具有军事意义上的必要性。军事必要性抬高了对于军民两用目标实施攻击的门槛，在军民两用目标的保护方面尤其具有价值。

通常而言，当目标满足军事性条件时，对其实施攻击一般都可以被认定为具有军事利益，但对于军民两用目标来说，其通常是作为一种可替代角色而出现的。倘若对其实施攻击不具有直观且现实的军事利益，在道德意义上就难以认定攻击具有合理性。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。[②] 对于目标的攻击若不影响军事活动的恢复能力，则此种目标不能受到攻击。军民两用目标倘若不存在“不可替代性”（irreplaceable），则不影响恢复能力，对其实施攻击也因此不具备充分的军事利益，因而不可对其实施攻击。对于上述问题，应当对其内涵进行严格解释，不应对军事利益的内涵进行推定或扩散。

在这方面，《塔林手册 2.0》给出了不良示例。其注解中指出：“一个兼具民用和军用的网络，不可能知道其哪一部分将用于军事通信传送，在这种情况下，整个网络符合军事目标的条件。”[③] 依据这一观点，任何网络目标都具备可攻击性，实质上是在允许网络领域的全面战争，这不符合当前国际社会约束战争的基本诉求。

还需要注意的问题是，军民两用目标作为网络攻击目标，在网络作战中可能提供军事利益，但其自身目的很可能并非用于军事利益。因此在判定军事利益方面，应以更高的人道主义保护标准考虑此类攻击目标的实际目的、用途。一些军事行动可能借由民事设施提供的公共服务而得以实现，对于此类民事设施实施的攻击行为应认为不具备充分的合理性。例如，在实施网络攻击的过程中，导致平民居民生存不可缺少的物体（如供电、供水设施和灌溉工程）失去效用，此类攻击应当被禁止。

（三）区分原则对于攻击者的行为规制

根据以上分析，在网络武装冲突中军民两用目标的“可攻击性”应当限于：此类目标存在对军事活动的现实贡献，且此类目标具有不可替代的军事利益。

由于当前有组织网络攻击的形式并非单一，以上判定需要以个案为出发点，从个案的整体过

---

① 《日内瓦公约第一附加议定书》第 52 条第 1 款规定：民用物体是指所有不是第 2 款所规定的军事目标的物体。

② 克努特·德尔曼、洛朗·吉塞勒、蒂尔曼·罗登霍伊塞尔：《国际人道法对网络战的可适用性及其适用》，丁玉琼译，载《国际法研究》2019 年第 4 期，第 15 页。

③ 《网络行动国际法塔林手册 2.0 版》规则 101 注解 4。参见〔美〕迈克尔·施密特等：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 433—434 页。

程来判断其发起攻击的合法性要件。若非“存在现实贡献且不可替代”，则对目标的攻击不具有充分的合理性。这一标准更适合作为裁判标准，而非行为标准，但倘若这一标准可以使冲突双方感到顾虑，那么在发挥人道主义保护的作用上便是有所作为的。

除了基于以上对军民两用目标的“可攻击性”判断之外，区分原则对军民两用目标的保护还体现在攻击者对自身攻击行为的控制力上，强调国家对自身攻击行为的“可控制性”。尤其军民两用目标在受到攻击时更易在民用层面上扩散，扩大攻击影响面，这在根本上是违背区分原则的。

网络攻击发起者每次发动攻击时都应查明，在当时的情况下，使用的网络武器是否能够确实针对所指向的目标，充分考虑军民融合背景下的“靶向”问题，以及其影响是否能够控制在国际人道法要求的范围内。即使再精准的网络攻击也无法完全保证不产生额外影响，空间“蝴蝶”效应[①]很好地描述了这种状况，因此只要其在攻击外观上满足精确、区分的特点即可。从各类实践中所观察到的攻击特点表明，网络攻击活动中的网络工具可以是特别精确定制的，只对特定的目标产生影响，因此有能力符合国际人道法原则和规则的要求。[②]

具体而言，攻击者不得使用性质上无法对目标加以区分的网络武器，对此类武器的应用应当在该武器的发展或对该武器进行审查的过程中被禁止，例如能够进行自我复制且不可能加以控制的病毒。在使用此类武器时，攻击者应当确保存在保护措施，并保证这种保护措施的有效性，如采取“系统围栏”“地理围栏”“紧急停止开关”等技术措施，[③] 使其能够在部署后控制传播。如果武器开始以其攻击者没有预料到的方式传播，这种保护措施应当确保攻击者在特定情况下仍然能够限制恶意软件造成的影响，限制其滥杀滥伤作用。即使在采取一些“非程式”的攻击时，如端口扫描、分布式拒绝服务攻击、安全漏洞等，实施攻击的形式也应当是“非溢出”（non-overflowed）的，最大程度上避免对非“可攻击性”目标的影响。

四　军民融合趋势下区分原则适用的立场与进路

以上对于军民融合背景下区分原则要件内涵的分析，旨在阐明区分原则在维持人道主义保护价值方面应有的标准，但此标准在当前的国际社会中并不易推行。在网络技术领域占据优势的国家更倾向于追求武装冲突法体系中的军事需要，忽视人道主义保护目标。为更好地维护国际法在网络空间的恰当适用，这一主题下的讨论，不仅是前述法律标准的探讨，还是规则话语权的探讨。

（一）网络空间国际法规则制定的基本立场

2021 年联合国大会决议指出：一些国家正在发展用于军事目的的信通技术能力；在未来的国家间冲突中使用信通技术的可能性越来越大。[④] 如今各国纷纷成立网络部队以应对网络武装冲

① 向宏：《从美军“网络战场建设”看网络空间作战能力的培养》，载《中国信息安全》2013 年第 1 期，第 72 页。

② 2020 年被发现的“太阳风”（solar winds）攻击集中体现了这一特点。这种攻击是一种极有针对性的、手动执行的攻击，而不是广泛的、系统范围的攻击。“太阳风”攻击体现出高度组织性，意味着国家层面有组织网络攻击在经过设计之后，是有可能在不影响非军事目标的前提下完成任务的。

③ “系统围栏”指的是在没有与目标系统实现精准匹配的情况下阻止恶意软件自动运行；“地理围栏”指的是将恶意软件的运行限制在特定的 IP 地址范围内；“紧急停止开关”指的是在一定时间后或遥控启动后关闭恶意软件。

④ 联合国大会：《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 7 月 14 日，第 7 段。

突的常态化。[①] 事实上，几个主要的互联网大国之间常年互相指责对方的网络攻击，其中由国家发起的攻击占据相当大的比例。然而各国在面对网络攻击时，多数情况下似乎仍选择沉默以对，因此目前难以从冲突中推断出关于区分原则等具体条款适用的法律立场。但可以从世界各国关于在网络空间中适用国际法的主张中窥得一些端倪。

从目前的公开发言来看，美国为首的西方国家总体上支持现有国际法在网络空间的适用，[②] 另有一些国家则偏向于在网络空间制定新的国际法规则。事实上，在国际人道法的适用方面，由于美国等国已在网络空间建立相当程度的技术优势，因此其关注传统国际人道法适用问题的目的在于取得实施网络武装冲突的合法性。对此，中国明确指出，确认（传统）武装冲突法适用于网络空间，相当于制定网络空间交战规则，无异于变相承认网络战的合法性，有可能会为一些国家发动网络战提供最后一片拼图。[③] 当上述立场分歧置于军民融合背景下时则更易理解。网络空间军民融合本质在于提升国防水平与社会发展水平，然而当前网络空间技术、资源、权限不对等，暗含着网络空间军民融合的两面性。对于美国而言，军民融合意味着其战略手段的延伸与强化；[④] 对其他国家而言，军民融合可能意味着网络设施被认定为军事目标的可能性大大增加，增加冲突受创面。

无论各国主张如何，其底层立场必须归于人道主义保护。近年来，各国的发展极大地受益于互联网，当遭受到国家级别的有组织网络攻击时经济发展将遭受严重损失，对于越来越多深度依赖互联网的国家尤其如此。[⑤] 对于各国来说，网络空间非冲突化应是当前的主要立场，是对《联合国宪章》原则的尊重与维护。即使当前在网络空间是否适用已有具体国际法规则的分歧尚未调和，但在网络空间适用《联合国宪章》已为绝大多数国家所确认。在此基础上应当明确的是，在网络空间制定新的国际法规则，其实质并非不愿遵守已有国际法，而是以网络空间非冲突化立场对冲网络武装冲突合法化立场。非冲突化的内核正是人道主义保护。在人道主义保护这一基本逻辑之上，无论是主张适用已有规则或是制定新规则，事实上都是并行不悖的。红十字国际委员会也指出："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。"[⑥] 两者最终都与《联合国宪章》基本精神相契合。

---

① 尽管仅少数国家公开承认曾使用网络手段支持其军事行动，但据估计，超过 100 个国家已经发展出或正在发展军事网络力量。参见"Cyber Warfare：Does International Humanitarian Law Apply?"，https：//www. icrc. org/en/document/cyber – warfare – and – international – humanitarian – law。

② Brian J. Egan，"International Law and Stability in Cyberspace"，https：//www. justsecurity. org/wp – content/uploads/2016/11/Brian – J. – Egan – International – Law – and – Stability – in – Cyberspace – Berkeley – Nov – 2016. pdf.

③ 《中国代表团团长王磊参赞在联合国信息安全开放式工作组首次会上关于国际法使用问题的发言》，http：//switzerlandemb. fmprc. gov. cn/web/gjhdq _ 676201/gjhdqzz _ 681964/lhg _ 681966/zyjh _ 681976/201910/t20191018 _ 9381633. shtml。

④ 美国立法限制私营企业私自展开网络攻击。私营企业可以提供技术和服务，但所有的攻击性网络作战行动必须由政府和国防部组织实施。这意味着在军民融合道路方面，美国私营企业已具备配合政府实施有组织网络攻击的能力，极大地强化了美国实施网络作战的作战能力。

⑤ 在网络攻击中，损害的严重程度并非客观且恒定，而是取决于不同的参数，如社会对某些网络系统的依赖性。See David Turns，"Cyber Warfare and the Notion of Direct Participation in Hostilities"，(2012) 17 *Journal of Conflict and Security Law* 279，p. 288.

⑥ 克努特·德尔曼、洛朗·吉塞勒、蒂尔曼·罗登霍伊塞尔：《国际人道法对网络战的可适用性及其适用》，丁玉琼译，载《国际法研究》2019 年第 4 期，第 9 页。

当前网络空间军事化发展日益严峻，在无法完全避免网络武装冲突的情势下，国际社会既要强调《联合国宪章》的基本原则适用于网络空间，以遏制网络武装冲突合法化趋势，也要探究国际人道法条款的适用性问题，以确保国家在真正被卷入到网络战争中时，正确合理地处理国际人道法在网络空间适用的诸多问题。《日内瓦公约第一附加议定书》序言奠定了分析这一问题的基础，该序言声明，国际人道法不得“解释为使任何侵略行为或任何与《联合国宪章》不符的武力使用为合法或予以认可”，这是国际社会探讨在网络空间中发展国际法规则的基本起点。

（二）区分原则适用于网络空间的实现进路

当前世界各个国家对于网络安全的需求只增不减，应对潜在的网络武装冲突已成为主要网络大国不得不关注的议题，尤其是涉及国际性武装冲突时。“网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这对世界各国都是一个难题，我们当然也不例外。”① 由于网络武装冲突实践在可观察到的范围内很少以大规模的形式存在，各国也因此极少对网络武装冲突的实践表示“法律确信”。如今国际社会完全不能确保武装冲突法主体以不违背现行国际法的方式来行事，在此情景下，探寻区分原则等重要的国际人道法原则适用的法理进路已然十分重要。

联合国信息安全政府专家组 2017 年未能就网络空间行为规范达成共识性文件，谈判破裂导致前景黯淡。② 联合国在约束网络武装冲突方面仍然无所作为，在部分决议文本中至多提及几项基本原则应予以考虑，除此以外再无更新的进展，对于区分原则具体如何适用没有给出进一步答案。由此得见，政府间专家组的工作受制于国家立场之间的分歧，短期内难有突破。

在非官方层面，“塔林手册”项目③的影响最为广泛。“塔林手册”参照一系列武装冲突的国际条约文本，系统阐述了传统国际人道法适用于网络空间的完整体系，俨然已成为网络战手册。“塔林手册”虽非官方文件，④ 然而，其编纂背景集中体现了欧美国家的立场，其追求规则话语权的目标是毋庸置疑的。经由精心的议程设置，“塔林手册”极有可能成为今后同类型国际规范的“路径依赖”。⑤ 在涉及区分原则适用的问题上，《塔林手册 2.0》版本中的部分观点直接将兼具军用和民用目的的网络基础设施认定为军事目标，这一观点与已有国际共识中对于民用设施的保护相背离，⑥ 亦与大多数国家的非冲突化立场相悖。事实上，红十字国际委员会以观察员的身份参与了专家小组的讨论，表示并不认同手册中的全部观点。⑦ 北约合作网络防御卓越中心（NATO Cooperative Cyber Defence Centre of Excellence）也希望通过更新版本来提升“塔林手册”

① 习近平：《论党的宣传思想工作》，中央文献出版社 2020 年版，第 201—202 页。

② 刘碧琦：《联合国“双轨制”下网络空间国家责任认定的困境与出路》，载《电子政务》2021 年第 2 期，第 101 页。

③ 此处“塔林手册”意指所有版本包括未来版本的手册，而非具体某一版本的手册。

④ 〔美〕迈克尔·施密特等：《网络行动国际法塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 48 页。

⑤ 正如一些观点所指出的，以“塔林手册”为代表的西方学说，表现出较为明显的“话语强权”色彩。参见黄志雄：《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》，载《现代法学》2015 年第 5 期，第 156 页。

⑥ 联合国决议明确指出，一国不应违反国际法规定的义务，从事或故意支持蓄意破坏关键基础设施或以其他方式损害为公众提供服务的关键基础设施的利用和运行的信通技术活动。参见联合国大会：《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 7 月 14 日，规范 13（f）。

⑦ Cordula Droege，“Get off My Cloud：Cyber Warfare，International Humanitarian Law，and the Protection of Civilians”，（2012）94 *International Review of Red Cross* 533，p. 541.

作为网络空间国际示范文本的地位，于2021年启动“塔林手册”3.0版本的编纂，说明其编纂者也认识到手册中诸多观点并非尽善尽美。

国际社会的当务之急在于确立网络武装冲突中的人道主义要求的实现路径，以更严格的标准适用区分原则。对此，国际社会应主张在现有基础上进行更加开诚布公地讨论，以便清楚地知道各国打算如何遵循区分原则。

其一，在区分原则适用性讨论的背景方面，应当重视红十字国际委员会在该领域的地位。红十字国际委员会在当前的各类武装冲突一线从事人道主义援助活动，其立场符合更广泛的人道主义保护的立场，[①] 如今在探讨如何约束政府武装力量和有组织武装团体不加区分地实施网络攻击方面也开始有所作为。[②] 在相关多边场合，支持红十字国际委员会发表观点，有利于区分原则等人道主义保护价值的实现。此外，其他国际组织在这一问题上的主张，也应当尽可能地与红十字国际委员会所追求的基本主旨相契合，在增进人道主义保护而非武装冲突的意义上讨论这一问题。

其二，在区分原则适用性讨论的立场方面，应当从网络空间命运共同体出发，强调在全球互联网连通的前提下，采取不加区分的网络武装冲突行动可能会遭到反噬。虽然一些国家凭借技术优势“相信其网络武器打击后果和范围可控，相信自己能成为网络冲突的赢家，相信凭借实力可将其霸权延伸至网络空间”，[③] 但是，现代社会各个国家的关键基础设施，经济、社会发展的方方面面均高度依赖网络，一旦爆发大规模国家间网络冲突，后果难以估算，范围难以控制。即使客观上确实存在网络攻击行为，此类行为也应当严格遵守区分原则。上述前提必须予以明确。

其三，在区分原则适用性讨论的举措方面，应当主张在非创新领域推行军民分离。对于网络技术更为成熟的国家，军民融合确实可以有效地协助国家增强网络空间整体的防护能力，但若一国不能在一定程度上达到以上目标，则应提倡本国民用目标的军事属性剥离，明示“数码安全区”，对外明确在网络武装冲突中不得攻击的民用目标，以确保非军事目标不被纳入攻击范围。所有国家必须尊重“数码安全区”应受保护的状态，不得加以攻击。此外，在推定意义上，对于“数码安全区”未纳入的民用目标应当采取更严格的认定标准，当民用网络要素并非真正参与作战时，原则上不可推定其具有军事属性。

五　结语

区分原则作为在武装冲突中实现人道主义保护的关键原则，其在网络武装冲突中的适用应当是国际社会安全议程予以优先讨论的议题。然而在军民融合趋势下，区分原则的适用愈发艰难，若对传统区分原则不加调试直接进行适用，便可能违背人道主义保护的基本需求。如今强调区分

① ICRC，“Cyber Operations during Armed Conflict are not Happening in a ‘Legal Void’ or ‘Grey Zone’ – They are Subject to the Established Principles and Rules of International Humanitarian Law”，https：//www. icrc. org/en/document/cyber – operations – during – armed – conflict – are – not – happening – legal – void – or – grey – zone – they – are.

② 参见红十字国际委员会官方网站，https：//www. icrc. org/en/war – and – law/conduct – hostilities/cyber – warfare。

③ 《中国代表团团长王磊参赞在联合国信息安全开放式工作组首次会上关于国际法使用问题的发言》，http：//switzerlandemb. fmprc. gov. cn/web/gjhdq _ 676201/gjhdqzz _ 681964/lhg _ 681966/zyjh _ 681976/201910/t20191018 _ 9381633. shtml。

原则在网络空间的适用，即是希望各个国家在满足自身网络空间军事需求，维护自身网络主权利益的同时，开始更多地考虑人道主义要求，避免在一个极端走得太远，而忽略考虑必不可少的另一端。

正如《联合国宪章》序言所言及："欲免后世再遭今代人类两度身历惨不堪言之战祸"，国际社会需要不断从惨痛的历史代价中探索追求国际法治的意义，并且就相关议题达成有效且坚实的合意。在这一背景下，网络武装冲突作为新情势下的对抗行为，已经从一些侧面显现出其招致战争的风险，因此，网络武装冲突相关国际法规则的发展刻不容缓。通过在有限的冲突实践中充分总结经验，并督促相关国家就这一问题明确立场，国际社会仍然有可能在这一领域实现冲突的有效管控，最终促使这一领域走向法治轨道。或许追求这一理想结果的道路并非坦途，但世界近代历史和《联合国宪章》已经在战争冲突方面带来足够的警示，这正是我们必须在这一问题上不断探索的理由所在。

On the Application of the Principle of Distinction in Cyber Armed Conflict Under the Trend of Military Civilian Integration

Jiao Yuanbo

Abstract: With the acceleration of the militarization of cyberspace all over the world, the application of the principle of distinction in cyber armed conflict is facing the challenge of military civilian integration. The military civilian integration trend mixes military and civilian attributes in nature, which is more likely to lead to indiscriminate cyber attacks. Accordingly, if the international community aims to apply the principle of distinction in cyberspace, it is necessary to analyze the balance of interests. At present, more attention should be paid to consider humanitarian requirements between military and humanitarian interests. In the dismantling and resetting of the principle of distinction, the "actual contribution" and "military interest" involved in the assaultable military targets should be interpreted strictly with the two aspects of "reality" and "irreplaceable", and strengthening the "controllability" of attacks. On the application of the principle of distinction in cyberspace, the international community should emphasize the nature of humanitarian protection, strengthen the status of the UN Charter, curb the trend of legalization of cyber armed conflicts, and realize humanitarian protection by encouraging reasonable military-civilian separation.

Keywords: Cyber Armed Conflict, Principle of Distinction, International Humanitarian Law, Military Civilian Integration, Tallinn Manual

(责任编辑：郝鲁怡)