ICRC

区分原则

区分原则要求武装冲突各方在使用信息和通信技术（信通技术）时，始终区分平民和战斗员，并区分民用物体和军事目标。网络攻击的对象只能是战斗员或军事目标，而不能是平民或民用物体。禁止不分皂白的网络攻击。

区分原则是国际人道法最古老的原则之一，也是国际人道法的基石。国际法院认为，这是一项“不可违背”的“基本”原则，是国际人道法“框架”的一部分。[1] 该项原则仅适用于武装冲突的情况，禁止攻击平民和民用物体。[2] 联合国政府专家组已经指出，在国际法如何适用于各国使用信通技术方面，区分原则是“既定的国际法律原则”之一，并认识到“需要进一步研究这些原则如何以及何时”适用。[3]

在武装冲突中使用信通技术时，**使网络攻击只针对军事目标而不针对民用物体的义务**尤为重要。在国际人道法上，民用物体被定义为一切不构成军事目标的物体。[4] 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。”[5] 这意味着不得攻击民用基础设施（包括供水站、发电站、私人财产，或民用政府信通技术设备和基础设施）或其它民用物体。在国际人道法上，将民用基础设施界定为“关键基础设施”不具有法律上的重要性。

区分原则是国际人道法框架中的一项基本原则。

在信通技术环境中，平民与军队通常使用同样的网络基础设施（例如光缆、卫星、路由器和网点），并可能依赖同样的数字通信、储存和其它服务。这种情况常被称为某物体的“军民两用”特征。将民用信通技术基础设施用于军事目的，可能会使该物体转变为军事目标。然而，实现这一转变需要同时满足上述两个条件：（1）该物体或基础设施的使用必须对军事行动有实际贡献，以及（2）其全部或部分毁坏、缴获或失去效用必须提供明确的军事利益。例如，尽管民用海底光缆可以被用于军事目的，但毁坏光缆是否能带来明确的军事利益仍有待商榷，因为通过这种电缆传输的数据可能通过重新路由到达接收者。另外，即使某一民用基础设施已经构成军用目标，任何对该目标的攻击都必须遵守其他国际人道法规则，尤其是比例原则和预防措施原则。如果网络空间的军事使用导致构成网络空间组成部分的许多物体不再受到免受攻击的保护，这将成为一个严重的问题，可能导致日益重要的信通技术民用服务遭到大规模破坏。[6]

1. ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, paras 78–79.
2. 1977年《第一附加议定书》第48条，第51条，第52条；红十字国际委员会，《习惯国际人道法研究》（2005年），规则1 及规则7。
3. 联合国，《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》，2021年7月，第71（f）段；另见联合国，《2021–2025年信息和通信技术安全和使用问题不限成员名额工作组报告》，2022年8月，第15（b）（二）段。
4. 1977年《第一附加议定书》第52条第一款；红十字国际委员会，《习惯国际人道法研究》（2005年），规则9。
5. 1977年《第一附加议定书》第52条第二款；红十字国际委员会，《习惯国际人道法研究》（2005年），规则8。
6. 红十字国际委员会，《国际人道法及其在当代武装冲突中面临的挑战》，2015年。

区分原则禁止不分皂白的攻击，包括采取网络作战手段或方法的攻击。不分皂白的攻击是指在性质上不加区分地打击军用目标和民用物体的攻击行为。[7] 这包括不以特定军事目标为对象的网络攻击，例如一项旨在清除敌方所有政府机关（包括民事机关和军事机关）的计算机内信息的网络行动；使用不能以特定军事目标为对象的作战手段或方法而进行的网络攻击，例如恶意软件利用民事和军事系统的漏洞，自我传播并释放至开放式网络中；以及使用其效果不能按照国际人道法的要求加以限制的作战手段或方法而进行的网络攻击，例如以某一军事目标作为对象，但一经释放，将无限制地传播，并可能对平民造成不成比例的伤害的网络行动。

哪些类型的网络行动构成“攻击”，受国际人道法关于敌对行动的所有规则约束，对此各国有不同看法。

网络行动存在诸多类型，并且**可以通过多种方式确保尊重区分原则**。例如，如果网络行动是由进入目标并针对该目标发起行动的操作人员执行的，操作人员通常知道自己的所在地和行为。因此，他们能够遵守区分原则。在其它情况下，网络行动可能通过恶意软件或其它网络工具开展。从技术角度而言，可以对网络工具进行编程，使其仅针对并伤害特定对象，而不是不分皂白地传播或造成伤害。然而，网络空间相互联通的特点意味着对一个特定系统的网络攻击也可能蔓延至其他系统，例如被设计为可蔓延至其他系统的网络工具或未经过充分测试的网络工具就可能导致上述情况。因此，网络工具的设计或使用——无论是故意为之还是意外导致——确实存在着不符合国际人道法的风险。

鉴于上述风险，正在计划或实施网络行动的人员必须采取一切可行措施，查明攻击目标为军事目标。[8] 这些手段应当包括，例如，仔细评估目标环境以及网络行动可能造成的影响；在与目标环境相似的信通技术环境中测试网络工具；以及采取“系统围栏”、“地理围栏”或“紧急停止开关”等技术措施，以预防或阻止网络工具不分皂白地传播及造成损害。[9]

国际人道法关于敌对行动的许多规则，包括源于区分原则的若干规则，[10]只适用于——并因此限制——构成国际人道法上的“攻击”（“不论在进攻或防御中对敌人的暴力行为”[11]）**的网络行动**。在网络行动的语境中，国际人道法上的攻击概念通常被理解为可合理预期将会造成人员伤亡或对物体造成损害或破坏的行动。[12] 目前，关于网络行动造成哪些类型的影响可被视为“损害”，从而使其构成国际人道法上的“攻击”，受到相关规则的限制，各国有不同看法。[13] 如采狭义理解，则可能意味着多种网络行动—例如破坏银行、民政管理或

7. 1977年《第一附加议定书》第51条第四款；红十字国际委员会，《习惯国际人道法研究》（2005年），规则11及规则12。
8. 1977年《第一附加议定书》第57条第二款第一项第1目；红十字国际委员会，《习惯国际人道法研究》（2005年），规则6。
9. “系统围栏”指的是防止恶意软件自我执行，除非与目标系统完全匹配；“地理围栏”指的是将恶意软件限制在特定的互联网协议范围内运行；而“紧急停止开关”则指在特定时间或远程激活后禁用恶意软件的一种方法。更多细节，请见ICRC, Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts, 2021, pp. 26–27。
10. 尤见1977年《第一附加议定书》第51条第四款及第五款第一项，第52条，第54条第三款，以及第57条第一款；红十字国际委员会，《习惯国际人道法研究》（2005年），规则7至规则11，规则14及规则15。
11. 《第一附加议定书》（1977年）第49条。需要注意的是，国际人道法规定了对某些物体的特殊保护，例如医疗设施、公正的人道组织或平民居民不可缺少的物体，这些物体享有的免受网络行动的保护范围不仅限于那些构成“攻击”的网络行动。
12. M. N. Schmitt and L. Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 92.
13. 关于各国对此所持立场的概述，见Cyber Law Toolkit, ‘Attack (international humanitarian law)’。

私营公司的信息技术系统但未造成实质性的物理损害的行为—可能不受相关国际人道法规则的限制。这一点实在令人担忧。红十字国际委员会认为，在武装冲突期间，旨在使计算机或计算机网络失效的行动，无论是采取动能手段还是网络手段，均构成国际人道法上的攻击。[14]

在武装冲突期间，不构成国际人道法上的“攻击”的网络行动仍然受到限制。例如，必要原则，经常注意不损害平民居民、平民和民用物体的义务，尊重并保护医疗设施和人道救济物资的义务，以及关于保护对平民居民生存所不可或缺的物品的规则适用于所有军事行动。[15] 此外，至少《第一附加议定书》的缔约国有义务“仅以军事目标为对象”开展行动。若将这一规则解释为允许网络行动针对民用物体，将难以与条约约文保持一致。[16]

---

14. 见红十字国际委员会，《国际人道法与武装冲突中的网络行动：红十字国际委员会立场文件》，2019年，第7～8页。
15. 尤见1949年《日内瓦第一公约》第19条；1977年《第一附加议定书》第12条，第54条第二款，第57条第一款，以及第71条；1977年《第二附加议定书》第13条第一款，第14条；红十字国际委员会，《习惯国际人道法研究》（2005年），规则15，25，28，29，32，54。
16. 1977年《第一附加议定书》第48条。

红十字国际委员会东亚地区代表处
中国北京市建国门外大街9号
齐家园外交公寓3-2
邮编：100600
电话：+86 10 8532 8500
传真：+86 10 6532 0633
邮箱：bej_beijing@icrc.org　www.icrc.org