ICRC

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

该文件已提交至“国际安全背景下信息和电信领域发展问题不限成员名额工作组”和“国际安全背景下促进网络空间负责任国家行为政府专家组”

2019 年 11 月

目录

内容摘要

- 在当代武装冲突中开展网络行动已成为现实。红十字国际委员会对武装冲突期间网络行动日益增多所带来的潜在人类代价表示担忧。

- 红十字国际委员会认为，就像国际人道法对武装冲突中任何其他新型或传统武器、作战手段和方法的使用进行限制一样，该法也对武装冲突期间的网络行动加以限制。

- 确认国际人道法可适用于网络战，并不代表这种作战形式的合法化，正如该法不能使任何其他作战形式合法化一样。各国任何动用（网络或动能）武力的行为仍受《联合国宪章》和相关习惯国际法相关规则，特别是禁止使用武力原则的规制。国际争端无论发生在网络空间还是在其他领域，均须以和平方式解决。

- 当前，由国际社会确认国际人道法可适用于武装冲突中的网络行动，已成为至关重要的工作。红十字国际委员会还呼吁政府专家和其他专家共同探讨如何在网络行动中适用现有国际人道法规则，以及现行法律是否充分到位。在这方面，红十字国际委员会乐于看到目前在联合国大会授权的两项进程框架内所开展的政府间讨论。

- 近年来的事件表明，网络行动无论是否在武装冲突中实施，均会严重影响重要民用基础设施的运转，阻碍向民众提供基本服务。在武装冲突局势中，现有国际人道法原则和规则，特别是区分原则、比例原则和攻击中的预防措施原则，保护民用基础设施免受网络攻击。国际人道法还为医院以及平民居民生存所不可缺少的物体提供特殊保护。

- 武装冲突期间，造成不分皂白的破坏的扩散型网络工具是禁止使用的。从技术角度来看，一些网络工具可设计用于仅攻击并破坏特定物体，但其不会扩散，也不会造成不分皂白的破坏。然而，网络空间的互联互通性意味着，可以从世界任意地点攻击任何与网络相联的物体，而且针对特定系统的网络攻击也可能影响其他各种系统。因此，网络工具在设计或使用上蓄意违反或因失误而违反国际人道法的风险是真实存在的。

- 各国对现有国际人道法规则的解释将决定国际人道法保护平民及民用物体免受网络行动影响的程度。各国尤其应明确承诺会对国际人道法做出积极解释，以保护民用基础设施不受重大破坏，并保护民用数据。这种立场也会影响对现行规则是否充分或是否需要制定新规的评估。如各国认为需要制定新规，则应以国际人道法等现有法律框架为基础并巩固该框架。

一、引言

在武装冲突中开展网络行动已成为现实。尽管只有少数国家公开承认实施过此类行动，但越来越多的国家正在发展军事网络能力，运用这一能力的情况或将不断增长。

而且，进攻性网络能力已取得重大技术进步：近年来的事件表明，网络行动可能会严重影响民用基础设施并造成人员伤亡。

红十字国际委员会根据其使命和职责，主要关注在武装冲突期间采用网络行动作为作战手段和方法的情况，以及国际人道法为平民和民用物体免受网络行动影响而提供的保护。

红十字国际委员会乐于看到目前在联合国大会授权的两项进程框架内所开展的政府间讨论，这两项进程分别是：“国际安全背景下信息和电信领域发展问题不限成员名额工作组”和“国际安全背景下促进网络空间负责任国家行为政府专家组”。这两个工作组的职责是研究“国际法如何适用于各国使用信息和通信技术的行为”。红十字国际委员会现已将本立场文件提交至上述两个工作组，以支持各国针对该问题进行审议。

本立场文件仅讨论武装冲突期间开展网络行动所引起的法律和人道问题，并不涉及非武装冲突中网络行动的法律框架适用问题。

二、网络行动的潜在人类代价

在武装冲突中，网络行动已用于支持或协助开展动能行动。网络行动可提供其他作战手段或方法无法实现的替代方案，但这种行动也带有一定风险。一方面，网络行动能够让武装冲突各方在既不伤害平民，又不对民用基础设施造成实际损害的前提下，实现其军事目标。而另一方面，近期网络行动（主要实施于非武装冲突中）表明，技术先进的参与方现已能够破坏对平民居民的基本服务供应。

通过网络行动，交战方可渗透到某一系统中收集、窃取、修改数据，或对数据进行加密或销毁；也可利用存在安全漏洞的计算机系统来触发、篡改或以其他方式操纵由该系统控制的进程。现实世界中的各种“目标”，如工业、基础设施、电信、运输、政府或金融系统，都可能受到干扰、篡改或破坏。基于与全球专家进行的讨论以及自身研究结果，红十字国际委员会日渐开始重视网络行动攻击医疗基础设施等重要民用基础设施时所造成的潜在人类代价。

近年来的网络攻击暴露出基础服务的脆弱性。据报道，此类攻击事件日益频繁且愈加严重，已超出专家预期。此外，我们仍对一些领域知之甚少：已研发成功或处于研发中的尖端网络能力和工具；技术演变方式；以及武装冲突中网络行动的开展与目前所观察趋势之间的差异程度。

另外，网络空间的特性也会引发特定问题。例如，网络行动可能会导致局势升级并造成人员伤亡，只因被攻击方可能难以获知攻击方是为了情报收集还是增加破坏。这会导致被攻击方出于对最差状况的预期而采取超过必要限度的过激应对措施。

网络工具的扩散方式也较为独特。网络工具一经使用，便可改变用途，并由原研发人员或用户以外的其他参与方广泛使用。

三、国际人道法在武装冲突期间网络行动中的适用

红十字国际委员会认为国际人道法无疑适用于武装冲突中的网络行动，并因此能够规制此类行动，正如该法对武装冲突中任何其他新型或传统武器、作战手段和方法的使用进行规制一样。无论网络空间被视为类似于陆海空及外太空的新作战领域，还是由于其人造属性不同于前者的自然属性而被视为完全不同的领域，抑或并非任何领域，国际人道法始终适用。

各国通过国际人道法条约的目的是规制当前和未来的冲突。各国在国际人道法条约中载明了一些预期新型作战手段和方法之发展的规则，推定国际人道法将适用于此类作战手段和方法。例如，如果国际人道法不适用于未来的作战手段和方法，那么就无需根据 1977 年 6 月 8 日《第一附加议定书》第 36 条的要求对其在现有国际人道法下的合法性进行审查。

这一结论可以在国际法院对《以核武器进行威胁或使用核武器的合法性》的咨询意见中找到有力佐证：国际法院回顾表示，适用于武装冲突的现有国际人道法原则和规则，同样适用于“所有作战形式和所有武器类型”，包括“未来的作战形式和武器”。红十字国际委员会认为，这项研究结论适用于武装冲突中实施的网络行动。

红十字国际委员会乐于看到越来越多的国家和国际组织确认国际人道法适用于武装冲突中的网络行动，并期待就国际人道法的适用方式开展讨论。

除现行法律规定外，各国可能还会决定对网络行动施加额外限制，并可能制定补充规则，特别旨在加强对平民和民用基础设施的保护，以抵御网络行动的影响。红十字国际委员会认为，任何正在构思的新规均需以国际人道法等现有法律框架为基础，并巩固该框架。

在不受现有国际人道法规则规制的情况下，平民和战斗员仍受“马顿斯条款”的保护，即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。

必须强调的是，确认国际人道法适用于武装冲突中的网络行动，并不代表将网络战合法化，也不是要鼓励网络空间军事化。实际上，国际人道法通过禁止发展可能违反国际人道法的军事网络能力，对网络空间的军事化施加了一些限制。此外，各国任何动用（网络和动能）武力的行为仍受《联合国宪章》和相关习惯国际法相关规则，特别是禁止使用武力原则的规制。国际争端无论发生在网络空间还是在其他领域，均须以和平方式解决。

四、现有国际人道法所提供的保护

现有国际人道法条约和习惯法通过大量条款规制武装冲突。就网络空间而言，规制敌对行动的规则尤为重要。这些规则旨在保护平民居民免受敌对行动影响，其基础是区分原则。这项根本原则要求交战方始终在平民居民与战斗员之间、民用物体与军用物体之间加以区分，并且仅针对军事目标实施打击。

尽管网络空间具有互联互通性，但仔细研究网络工具的运行，就能发现这些工具未必不分皂白。近期公开报道的多起网络攻击就技术角度而言似乎均实现了对攻击目标的精准识别：其中所涉及的网络工具仅设计用于攻击并破坏特定物体，但其不会扩散，也不会造成不分皂白的破坏。然而，确保仅攻击特定目标可能存在技术挑战，而且还需在制定和开展网络行动时进行审慎规划。另须指出的是，无论是否发生在武装冲突期间，在技术层面可以区分攻击目标的网络行动未必都是合法行动。

即使如此，也确实有一些网络工具设计为自我繁殖式工具，可以不分皂白地影响广泛使用的计算机系统。这种情况并非偶然：自我繁殖的能力是在设计此类工具时需要专门加入的。网络空间的互联互通性意味着，可以通过网络从世界任意地点攻击任何与网络相联的物体。而且，针对特定系统的攻击也可能影响其他各种系统，造成滥杀滥伤的后果。因此，网络工具在设计或使用上蓄意违反或因失误而违反国际人道法的风险是真实存在的。

确认国际人道法（包括区分原则、比例原则和预防措施原则）适用于武装冲突中的网络行动，意味着根据现行法律，应遵循一系列规则，例如：

- 禁止使用构成武器且具有不分皂白性质的网络能力。
- 禁止针对平民和民用物体实施攻击，采用网络作战手段或方法时也是如此。
- 禁止以在平民居民中传播恐怖为主要目的实施暴力行为或以暴力相威胁，采用网络作战手段或方法时也是如此。
- 禁止不分皂白的攻击，即禁止对军事目标与平民或民用物体不加区分地实施攻击，采用网络作战手段或方法时也是如此。
- 禁止不成比例的攻击，采用网络作战手段或方法也是如此。不成比例的攻击是指，与攻击预期获得的具体和直接军事利益相比，可能会造成过分的附带平民伤亡和（或）民用物体毁损的攻击。

- 在军事行动中，包括在使用网络作战手段或方法时，必须始终注意保护平民居民和民用物体；必须采取一切可行的预防措施，避免或至少尽量减少攻击所造成的附带平民伤害，采取网络作战手段和方法时也是如此。

- 禁止对平民居民生存所不可缺少的物体进行攻击、毁坏、清除或使其失去效用，采取网络作战手段和方法时也是如此。

- 医疗服务必须得到保护和尊重，在武装冲突中开展网络行动时也是如此。

此外，各国在和平时期必须履行的一项义务是，必须采取一切可行的预防措施，保护平民和民用物体免受采用网络作战手段和方法的攻击的影响。可考虑采取的措施包括：将军用网络基础设施和网络从民用网络基础设施和网络中分离；将重要民用基础设施所依赖的计算机系统从互联网中分离；努力确定专门保护医院等物体的网络基础设施和网络。

五、探讨国际人道法适用方式的必要性

确认国际人道法适用于武装冲突中的网络行动是避免或尽量减少网络行动可能造成的人类苦难的首要步骤。此外，红十字国际委员会还鼓励各国就国际人道法的原则和规则如何适用于网络行动达成共识。此项工作十分必要，因为网络空间的互联互通性及其数字化特征为解释国际人道法有关敌对行动的主要原则和概念带来了挑战。

在本立场文件中，红十字国际委员会将重点阐述三个相关问题。

网络空间的军事利用及其对网络空间民用性质的影响

除了一些特定军用网络外，网络空间以民用为主。不过，民用网络和军用网络可能相互联接；军用网络可能会依赖海底光缆、卫星、路由器或节点等民用网络基础设施。另一方面，民用车辆、航运和空中交通管制日益依赖卫星导航系统，而这些系统也可能为军方所用。民用物流供应链和重要民用服务与一些军事通信手段使用同一网络和通信网络。

将民用物体用于军事目的并不使该物体自动成为国际人道法规定的军事目标。然而，如果民用物体变为军事目标，那么该物体则不再受禁止攻击民用物体这一规定的保护。如果网络空间的军事利用导致构成该空间的许多物体不再作为民用物体得到保护，那么这将引发严重问题，可能会对日益重要的民用网络空间造成大规模破坏。

然而，即使在武装冲突期间，网络空间基础设施的某些部分不再作为民用物体受到保护，针对这些设施的所有攻击也仍然继续受禁止不分皂白攻击的规则、比例原则以及攻击中的预防措施原则的规制。正是因为民用网络和军用网络联系极为紧密，评估网络行动可能造成的附带平民伤害对确保平民免受其影响才至关重要。

国际人道法中的“攻击”概念与网络行动

能够提供基本服务的重要民用基础设施日益依赖数字化系统。因此，保护此类基础设施和服务免受网络攻击或附带损害对于保护平民居民至关重要。

无论在何种攻击行动中，国际人道法均为某些基础设施提供特殊保护，如医疗服务和民众生存所不可或缺的物体。然而，大多数源自区分原则、比例原则和预防措施原则，并为平民和民用物体提供一般保护的规则，仅适用于国际人道法界定为“攻击”的军事行动。《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”。因此，就网络行动而言，对“攻击”这一概念在何种程度上进行广义或狭义解释，对于这些规则的适用及其对平民和民用基础设施的保护至关重要。

人们普遍认为，预期造成人员伤亡或实际损害的网络行动在国际人道法中均构成攻击行为。红十字国际委员会认为，此类攻击行为包括因可预见的直接和间接（或衍生）影响而造成伤害的网络行动：例如，网络行动针对电网实施攻击，造成医院电力供应中断，继而导致医院重症监护室患者死亡的情况。

除此之外，严重破坏基本服务但未必造成实际损害的攻击是平民面临的重大风险之一。然而，对于导致基本服务无法运转但并未造成实际损害的网络行动是否构成国际人道法中的攻击行为，人们持有不同意见。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去效用的动能或网络行动均构成国际人道法中的攻击行为。如果仅将攻击解释为造成人员伤亡或实际损害的行为，那么旨在使民用网络（如电力供应、银行业务或通信网络）无法运转或预期造成此类附带影响的网络行动，则可能不受保护平民居民和民用物体的国际人道法基本规则的规制。对攻击概念的这种狭义解释很难与国际人道法有关敌对行动规则的目的和宗旨相一致。因此，为确保充分保护平民居民免受网络行动的影响，各国必须对攻击的概念达成共识。

民用数据与“民用物体”的概念

重要民用数据是数字化社会的重要组成部分，其中包括医疗数据、生物测定数据、社保数据、税务记录、银行账户、公司客户档案或选举名单和记录等。对个人和整个社会而言，此类数据均关系到大部分平民生活的正常运转。因此，保护这类重要民用数据已成为人们日益关注的问题。

国际人道法提供的一些特殊保护也延伸覆盖重要数据。例如，由于法律规定应履行尊重和保护医疗机构的义务，医疗机构所掌握的相关数据也受到保护。

更广泛而言，规制敌对行动的主要国际人道法原则和规则保护平民和民用物体。因此，各国必须承认民用数据受这些规则的保护。

删除或篡改重要民用数据可迅速导致政府服务和私营企业完全陷入瘫痪，其对平民所造成的伤害远远超出对实际物体造成的破坏。民用数据是否以及在何种程度上构成民用物体仍是一个有待解决的问题。红十字国际委员会认为，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此类重要民用数据的主张似乎难以与国际人道法的目的和宗旨相一致。纸质文件和资料即使由数据形式的数字文件取代，也不应减少国际人道法对它们的保护。将重要民用数据排除在国际人道法对民用物体的保护之外，将导致在保护方面出现重大缺口。

六、从国家责任角度看网络行为的归因问题

网络空间为参与方隐藏或篡改身份提供了各种技术可能性，这导致归因问题更为复杂并带来重大挑战。例如，即使在武装冲突期间，国际人道法也仅适用于与冲突有关的行动。如果无法确定网络行动的实施者，并因此无法确定该行动与所涉武装冲突之间的联系，则难以判定国际人道法是否适用于该行动。网络行动的归因问题也关系到能否确保向违反国际法（包括国际人道法）的参与方追究责任。认为网络攻击责任易于推卸的观点可能削弱对网络攻击的禁忌，并导致参与方在违反国际法，开展网络攻击方面采取更为放纵的态度。

即便如此，归因问题并不会给实施、指挥或控制网络行动的参与方造成困难：他们已掌握所有相关事实，可据此确定其行动应受何种国际法框架规制，以及应遵守哪些义务。

根据国际法，一国应对可归因于该国的行为负责，包括可能违反国际人道法的行为。这包括：

- 国家机关实施的行为，包括其武装部队或情报机构的行为；
- 有权行使某些政府职权的个人或实体的行为，如私营公司的行为；
- 事实上按照国家指示或在该国指挥或控制下行事的个人或团体的行为，如民兵或黑客团体的行为；以及
- 国家承认并当做自身行为的个人或私营团体的行为。

这些原则适用于通过网络或任何其他手段实施的行为。

七、结论

在武装冲突期间，采用网络行动的作战手段或方法可能给平民造成伤害。为保护平民居民和民用基础设施，必须承认此类行动也受法律规制。红十字国际委员会敦促各国重申国际人道

法对武装冲突中网络行动的适用性，并表明这种确认既不鼓励网络空间军事化，也不会使网络战合法化。

与此同时，红十字国际委员会认为，各国之间尤其需要进一步探讨如何在网络空间中解释和适用国际人道法。现在亟需开展此类讨论，因为决定发展或获取可构成武器及作战手段和方法之网络能力的国家，无论是出于进攻还是防御目的，都必须确保在使用这些网络能力时遵守国际人道法所规定的义务。这些讨论应基于对军事网络能力发展、潜在人类代价以及现有法律保护的深入理解。各国需要确定现行法律是否足以应对网络空间互联互通性和数字化特征所带来的挑战，或者是否必须进行调整以适应网络空间的特定特征。若要制定新规则来保护平民免受网络行动的影响，或出于其他原因保护平民，则应以国际人道法等现有法律框架为基础并巩固该框架。

红十字国际委员会乐于看到目前在联合国大会授权的两项进程框架内所开展的政府间讨论，并感谢有机会与参与各国交流意见。红十字国际委员会还时刻准备在各国认为适当的情况下，为此类讨论贡献其专业知识。