

国际人道法何时适用于信息和通信技术（信通技术）的使用？

国际人道法适用于武装冲突局势中信通技术的使用

许多国家和非国家武装团体已经发展或正在发展网络军事能力，在武装冲突期间开展网络行动已成为现实。

出于法律和人道原因，确定国际人道法“何时”适用于信通技术的使用，具有重要意义。这决定了交战方在开展网络行动时，在哪些情况下需要遵守国际人道法的原则和规则，并对可能违反国际人道法的行为（包括构成战争罪的行为）承担法律责任。国际人道法的目的和宗旨是“保护武装冲突受难者”。¹

在国际人道法上，确定何时存在武装冲突的唯一目的，就是判定国际人道法是否适用。这个结论的作出，并非基于政治评估，而是基于法律评估。日内瓦四公约以及其他国际人道法规则的适用是基于客观标准，而非取决于“宣战”或其他政治行为。²此外，判定国际人道法何时适用，与判定某一行为是否构成《联合国宪章》禁止的“使用威胁或武力”或《联合国宪章》中规定的“武力攻击”，是两个不同的法律问题。³普遍公认的观点是，重申及适用国际人道法规则和原则“绝不是要给冲突披上合法外衣或鼓励冲突”。⁴

关于敌对行动的国际人道法规则仅适用于武装冲突局势。

国际人道法仅适用于武装冲突局势。国际人道法将武装冲突分为两类，即国际性武装冲突和非国际性武装冲突。应采取何种标准来判定国际人道法何时适用，取决于武装冲突的类型。

1. 1977年《第一附加议定书》序文。
2. 1949年日内瓦四公约，共同第二条和共同第三条。另见ICRC, Commentary on the Third Geneva Convention, 2020, commentary on Article 2, para. 227.
3. 见1945年《联合国宪章》第2条第4款和第51条。
4. 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（GGE报告），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；1977年《第一附加议定书》序文。

国际人道法适用于国家之间所发生的“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。”⁵ 普遍认为，“只要发生国家之间诉诸武力的情况，即存在武装冲突”。⁶ 判定国际人道法何时适用于两个或两个以上国家之间的网络行动，应分情况进行分析：

1. 若一国对另一国发起的网络行动是在已经存在的武装冲突的背景下，与“物理的”或“动能的”传统军事行动相结合或为其提供支持，那么国际人道法适用于该网络行动。⁷
2. 若一国对另一国发起网络行动时，两国之间并不存在武装冲突，而网络行动是开展敌对行为的唯一手段，在这种情况下该网络行动是否能构成日内瓦四公约共同第二条所定义的国际性武装冲突，法律尚无定论。

专家总体上同意：具有与传统动能军事行动类似效果的网络行动将构成国际性武装冲突，该网络行动也因此受国际人道法相关规则的限制。⁸ 这也是部分国家以及红十字国际委员会所持的观点。也就是说，如果甲国发起的网络行动，旨在或预期使乙国的民用工业厂房起火，造成人员伤亡和财物损失，该网络行动就构成国际性武装冲突，受国际人道法调整；而甲国的行为，一如使用导弹袭击民用工厂的行为，也会构成对国际人道法的违反。此类网络行动还可能构成对《联合国宪章》的违反。

国际人道法适用于在已经存在的武装冲突的背景下，与“物理的”或“动能的”传统军事行动相结合或为其提供支持的网络行动。

然而，对军事或民用基础设施进行干扰，但不对其造成物理破坏或损害的网络行动是否会构成国际性武装冲突，对于这一问题法律尚无定论。各国是否将此类网络行动——例如在不造成物理损害或人员伤亡的情况下，干扰另一国关键基础设施的运行——视为两国之间诉诸武力，以及在何种情况下将其视为诉诸武力，从而受到国际人道法的规制，仍有待观察。

在国际人道法上，“政府当局与有组织的武装团体之间，或一国境内的有组织的武装团体之间旷日持久的武装暴力”构成**非国际性武装冲突**。⁹ 在非国际性武装冲突的背景下，国际人道法何时适用，需要区分以下两种情况：

1. 若一国或一个非国家武装团体开展网络行动是在已经存在的武装冲突期间，与“物理的”或“动能的”传统军事行动相结合或为其提供支持，那么国际人道法就适用于该网络行动。
2. 若并不存在既有的武装冲突，一国或一个非国家武装团体开展的网络行动，只有在满足了与动能暴力构成非国际性武装冲突相同的标准时（即暴力需达到一定的强度，且须在至少两个达到一定组织性的当事方之间发生），此类网络行动才构成非国际性武装冲突。¹⁰

5. 1949年日内瓦四公约，共同第二条。

6. ICTY, Tadić Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 70; ICRC, Commentary on the Third Geneva Convention, 2020, commentary on Article 2, para. 218.

7. Ibid. para. 287.

8. 见Ibid. para. 288. 各国对此所持立场的概述，见Cyber Law Toolkit, “International armed conflict”. See also 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.

9. ICTY, Tadić Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 70.

10. ICRC, Commentary on the Third Geneva Convention, 2020, commentary on Article 3, para. 455.

鉴于当前的技术现状，如果一国与一个有组织武装团体之间，或不同有组织武装团体之间的敌对行动完全由网络行动组成，则不太可能达到国际人道法所要求的暴力的激烈程度。¹¹ 例如，非国家行为方开展的干扰或损害关键基础设施的网络行动（或其他形式的“网络犯罪”）本身不构成非国际性武装冲突，因而不受国际人道法的调整。

无疑，关于敌对行动的国际人道法规则不适用于武装冲突局势之外的情形。¹² 这一点很重要，因为国际人道法的规则和原则是针对武装冲突这一特定局势而商定的，并不针对和平时进行适用。在不存在武装冲突的情况下，国家之间的争端仅由其他领域的国际法进行调整，例如《联合国宪章》和可适用的人权法。

11. 各国对此所持立场的概述，见Cyber Law Toolkit, “Non-international armed conflict”.

12. 正如联合国政府专家组在2021年指出：“国际人道法仅适用于武装冲突局势”。见《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》，第71(f)段。但需要注意的是，为确保在发生武装冲突时尊重国际人道法，在和平时期须采取某些措施，例如对国际人道法进行传播和培训，为实施国际人道法进行某些国内立法，对新武器、作战手段和方法进行法律审查，或采取措施保护平民免受攻击影响等。

13. 见1945年《联合国宪章》第2条第4款，第42条和第51条。