

WHEN DOES INTERNATIONAL HUMANITARIAN LAW APPLY TO THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES?

International humanitarian law applies to the use of information and communications technologies in situations of armed conflict.

As a number of States and non-State armed groups have developed – or are developing – military cyber capabilities, the use of cyber operations during armed conflict has become a reality.

Determining ‘when’ international humanitarian law (IHL) applies to the use of information and communications technologies is important for legal and humanitarian reasons. It determines when belligerents have to comply with IHL principles and rules in the conduct of cyber operations and bear legal responsibility for possible violations of IHL, including for war crimes. The object and purpose of IHL is to ‘protect the victims of armed conflict’.¹

Under IHL, assessing when an armed conflict exists has the sole purpose of ascertaining if IHL applies. It is not a political assessment but a legal one. The Geneva Conventions and humanitarian law more generally apply based on objective criteria.² Their application does not depend on a ‘declaration of war’ or another political act. Moreover, determining when IHL applies is legally distinct from the question of which conduct amounts to a prohibited ‘threat or use of force’ or an ‘armed attack’ under the UN Charter.³ It is widely agreed that recalling – and applying – IHL rules and principles ‘by no means legitimizes or encourages conflict’.⁴

IHL rules on the conduct of hostilities apply only in situations of armed conflict.

International humanitarian law applies only in situations of armed conflict. IHL differentiates between two types of armed conflicts, namely international armed conflicts and non-international armed conflicts. The criteria for determining when IHL applies depend on the type of conflict.

¹ Additional Protocol I (1977), preamble.

² Geneva Conventions (1949), common Articles 2 and 3. See also ICRC, *Commentary on the Third Geneva Convention*, 2020, commentary on Article 2, para. 227.

³ See UN Charter (1945), Articles 2(4) and 51.

⁴ UN, *Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security*, July 2021 (GGE report), para. 71(f); see also UN, *Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*, August 2022, para. 15(b)(ii); Additional Protocol I (1977), preamble.

Between States, IHL applies ‘to all cases of declared war or of any other armed conflict [...], even if the state of war is not recognized by one of them’.⁵ It is widely understood that ‘an armed conflict exists whenever there is a resort to armed force between States’.⁶ To determine when IHL applies to cyber operations between two or more States, the following cases should be differentiated:

1. When a cyber operation is carried out by one State against another in conjunction with or in support of classic ‘physical’ or ‘kinetic’ military operations in the context of an existing armed conflict, IHL applies to such operations.⁷
2. If – *outside* an existing armed conflict – a cyber operation is the only means by which hostile actions are undertaken by one State against another State, the law is unsettled as to whether such cyber operation could bring into existence an international armed conflict as defined under Article 2 common to the Geneva Conventions.

Experts generally agree – and several States as well as the ICRC have taken the view – that cyber operations having similar effects to classic kinetic operations would bring into existence an international armed conflict and therefore be limited by the relevant IHL rules.⁸ Thus, a cyber operation by State A designed or expected to cause a civilian industrial plant in State B to catch fire, causing human and material loss, would in itself be an international armed conflict governed by IHL, and be a violation thereof – in the very same way as a missile strike on such factory would. Such operation may also violate the UN Charter.

IHL applies when a cyber operation is carried in conjunction with or in support of classic ‘physical’ or ‘kinetic’ military operations in the context of an existing armed conflict.

In contrast, the law is uncertain on whether a cyber operation that disrupts military or civilian infrastructure without physically destroying or damaging it would bring into existence an international armed conflict. It remains to be seen if and under what conditions States treat such cyber operations – for example, disrupting the functioning of critical infrastructure in another State without causing physical damage, or injury and death of people – as a resort to armed force between two States and as such regulated by IHL.

Under IHL, a **non-international armed conflict** exists if there is ‘protracted armed violence between governmental authorities and organized armed groups or between such groups within a State’.⁹ To determine when IHL applies in the context of such conflicts, two situations should be distinguished:

1. When a cyber operation is carried out by a State or a non-State armed group in conjunction with or in support of classic ‘physical’ or ‘kinetic’ military operations during an existing non-international armed conflict, IHL applies to such operations.
2. Outside an existing armed conflict, cyber operations carried out by a State or non-State armed group will amount to a non-international armed conflict only if they satisfy the same criteria that apply with regard to kinetic violence (i.e. violence needs to have reached a certain intensity and it must be between at least two organized parties).¹⁰

In light of the current state of technology, if hostilities between a State and an organized armed group, or between such groups, consist exclusively of cyber operations, the intensity of violence as required under IHL is unlikely to be reached.¹¹ For example, a cyber operation by a non-State actor disrupting or damaging critical infrastructure (or other forms of ‘cybercrime’) will not, in and of itself, amount to a non-international armed conflict and will therefore not be subject to IHL.

⁵ Geneva Conventions (1949), common Article 2.

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 See *ibid.* para. 288. For an overview of positions taken by States on this subject, see 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.

¹¹ For an overview of positions taken by States on this subject, see Cyber Law Toolkit, ‘[Non-international armed conflict](#)’.

It is undisputed that IHL rules on the conduct of hostilities do not apply outside situations of armed conflict.¹²

This is important because IHL rules and principles have been agreed for the specific situation of armed conflicts – not for application in times of peace. Outside an armed conflict, disputes among States are solely regulated by other fields of international law, such as the UN Charter and human rights law, as applicable.¹³

¹² As the UN Group of Governmental Experts noted in 2021: ‘international humanitarian law applies only in situations of armed conflict’. See GGE Report, para. 71(f). Note, however, that certain measures must be taken in peacetime in order to ensure respect for IHL in the event an armed conflict occurs, such as the duties to disseminate and train IHL, to adopt certain implementing domestic legislation, to carry out legal reviews of new weapons, means and methods of warfare, or to take measures to protect civilians against the effects of attacks.

¹³ See UN Charter (1945), Articles 2(4), 42, and 51.