Norway

# NORWEGIAN POSITIONS ON SELECTED QUESTIONS OF INTERNATIONAL LAW RELATING TO CYBERSPACE

**May 2021**

## 1. Introduction

International law applies in cyberspace. This has been recognised by the international community. The 2012-2013 United Nations Group of Governmental Experts (GGE)[1] concluded as much in its consensus report, and wrote as follows:

> *'International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.'*[2]

This was reconfirmed in the subsequent consensus report by the 2015 GGE, which also underscored that the UN Charter applies in its entirety.[3] The UN General Assembly welcomed the 2015 report of the GGE in its resolution 70/237 and called upon Member States to be 'guided in their use of information and communications technologies' by the report.

In the Final Substantive Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), all UN Member States reaffirmed the conclusions of previous GGEs that international law applies in cyberspace.[4] Moreover, the report called upon States 'to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations.' The report also concluded that 'further common understandings need to be developed on how international law applies to State use of ICTs.'

Compliance with international law is fundamental for preserving international peace and security in cyberspace. In this paper, Norway sets out its views on the concrete application of certain rules of international law to State conduct in cyberspace, including practical examples, to contribute to a common understanding among States.

The focus of this paper is on cyber activity that threatens international peace and security, and on issues of State sovereignty. However, numerous bilateral and multilateral treaties are also binding on States, and cyber activity perpetrated by or attributable to a State also has the potential to violate such obligations.

[1] UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.

[2] See UN Doc., 24 June 2013, A/68/98*, para. 19.

[3] See UN Doc., 22 July 2015, A/70/174.

[4] See UN Doc., 12 March 2021, A/AC.290/2021/CRP.2 para. 34.

## 2. The application of international law in cyberspace

**Key message:**
**International law applies in cyberspace.**

Existing international law, that is customary international law and international treaties, has not been developed with cyberspace in mind. However, the application of the rules of international law to new areas, for example in response to technological developments, is nothing new. If the law in certain areas is perceived as unclear when applied to activities in cyberspace, this must be resolved in the usual way through interpretation. This applies both to general international law, for instance the rules that relate to sovereignty and state responsibility, and to the specialised regimes of international law, such as international human rights law and international humanitarian law.

Norway is of the view that there is no need for specific legal instruments to set out rights and obligations of States in respect of activities in cyberspace.

## 3. Cyber operations in violation of international law

**Key message:**
**One of the conditions for holding a State internationally responsible for a cyber operation is that the operation, or the failure to react against the operation, constitutes a breach of an international obligation of the State.**

Cyber operations can vary widely in scope and intensity, from minor digital disruptions to armed attacks on a State. One of the conditions for holding a State internationally responsible for a cyber operation is that the operation, or the failure to react against the operation, constitutes a breach of an international obligation of the State.[5] The obligation in question may follow from customary international law or be treaty-based. A cyber operation is thus not unlawful *per se* but may become so when carried out to the detriment of the rights of other States.

In the following, Norway gives its interpretation of certain obligations of international law as they apply to cyber operations.[6] The focus in Section 3 is on sovereignty, non-intervention and the prohibition on the use of force. The question of attribution of conduct to a State, which is the other condition for holding a State internationally responsible for a cyber operation, is dealt with in Section 4 (*State responsibility*). The measures a targeted State is entitled to use in response under international law are dealt with in Section 5 *(Response measures).* Section 6 discusses international humanitarian law as it applies to cyber operations in armed conflict, and Section 7 deals with the application of international human rights obligations in cyberspace.

[5] This is set out as one of two conditions in Article 2 of the International Law Commission's Articles on State Responsibility (ILC ASR). The Article is considered to express customary international law.

[6] This position paper does not contain any specific analysis of cyber espionage, that is cyber operations whose purpose and effect is limited to the mere collection of information for use by the authorities, which is not in itself illegal under international law. However, certain aspects of such intelligence operations could violate specific rules of international law.

## 3.1 Sovereignty

**Key message:**
**Sovereignty is not just a principle, but also a primary rule of international law.**

**A State must not conduct cyber operations that violate another State's sovereignty.**

**Whether a cyber operation violates the target State's sovereignty depends on the nature of the operation, the scale of the intrusion and its consequences, and must be assessed on a case-by-case basis.**

The principle of sovereignty is one of the fundamental principles of international law and applies in cyberspace.[7] It refers to the supreme authority of every State within its territory to the exclusion of other States, and also in its relations with other States.

The internal dimension of a State's sovereignty includes the exclusive right to exercise jurisdiction within its territory, including over the information systems located on its territory, and to exercise independent State powers. The external dimension includes the right of the State to decide its foreign policy and to enter into international agreements. Both dimensions of sovereignty apply in cyberspace, subject only to obligations under international law.

Norway is of the view that sovereignty constitutes both an international law *principle* from which various rules derive, such as the prohibition of intervention and the prohibition of the use of force, and a primary *rule* in its own right capable of being violated.[8] Thus, cyber operations that do not amount to a prohibited intervention or a prohibited use of force may nevertheless amount to a violation of a State's sovereignty under international law.

The International Court of Justice (ICJ) has consistently held that States have an obligation to respect the territorial integrity and political independence of other States as a matter of international law. In a cyber context this means that a State must not conduct cyber operations that violate another State's sovereignty.

**A cyber operation that manifests itself on another State's territory may, depending on its nature, the scale of the intrusion and its consequences, constitute a violation of sovereignty**.

Causing physical damage by cyber means on another State's territory may easily qualify as a violation of territorial sovereignty. For example, a cyber operation against an industrial control system at a petrochemical plant that led to a malfunction and a subsequent fire would constitute a violation of the State's territorial sovereignty. In addition to physical damage, causing cyber infrastructure to lose functionality may also be taken into consideration and may amount to a violation. This includes the use of crypto viruses to encrypt data and thus render them unusable for a substantial period of time.
The principle of sovereignty encompasses cyber infrastructure located in a State's territory irrespective of whether it is governmental or private.

[7] *Island of Palmas case (USA v Netherlands),* arbitral award, 4 April 1928: *'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State',* p. 838.
[8] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 'Nicaragua case'*, International Court of Justice (ICJ), judgment 27 June 1986, paras. 15, 212-213 and 292.

**Similarly, a cyber operation that interferes with or usurps the inherently governmental functions of another State may constitute a violation of sovereignty.[9]**

This is based on the premise that a State enjoys the exclusive right to exercise within its territory, 'to the exclusion of any other State, the functions of a State'.[10] Accordingly, what matters is not whether physical damage, injury, or loss of functionality has resulted, but whether the cyber operation has interfered with data or services that are necessary for the exercise of inherently governmental functions. Cases in point would include altering or deleting data or blocking digital communication between public bodies and citizens so as to interfere with the delivery of social services, the conduct of elections, the collection of taxes, or the performance of key national defence activities. Another example could be the manipulation of police communications so that patrol cars are unable to communicate with police dispatch/operation centres. In this context it is irrelevant whether the inherently governmental function is performed by central, regional or local governments and authorities, or by non-governmental bodies in the exercise of powers delegated by such governments or authorities. Conducting elections is a clear example of an inherently governmental function. In contrast to the case of a cyber operation in breach of the prohibition of intervention, there is no requirement for the interference to reach to the level of coercion.

The precise threshold of what constitute a cyber operation in violation of sovereignty is not settled in international law, and will depend on a case-by-case assessment.

## 3.2 The prohibition of intervention

> **Key message:**
> **Cyber operations that compel the target State to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued (coercion) in matters relating to its internal or external affairs (*domaine réservé*), will constitute an intervention in violation of international law.**

The prohibition of intervention applies to a State's cyber operations as it does to other State activities.[11] Accordingly, a State must not carry out cyber operations in breach of the prohibition of intervention, according to customary international law.[12]

A cyber operation must therefore not be carried out to compel the target State to take a course of action, whether by act or omission, in a way that it would not otherwise voluntarily have pursued (coercion) in matters relating to its internal or external affairs (*domaine réservé*) – such as a State's political, economic, social or cultural system or the formulation of its foreign policy.[13] The constituent element of coercion means that cyber activities that are merely influential or persuasive will not qualify as illegal intervention.

Holding elections is an example of a matter within a State's *domaine réservé*. Thus, carrying out cyber operations with the intent of altering election results in another State, for example by manipulating election systems or unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak'), would be in violation of the prohibition of intervention. Another

[9] See Tallinn Manual 2.0, commentary to Rule 4, p. 21-22, paras. 15-16.

[10] *Island of Palmas* arbitral award, p. 838.

[11] Norway recognises that no State seems to object to the application of the prohibition on intervention (or rule of non-intervention) in the cyber context. Reference is made to the GGE 2015 report, para. 26 and 28(b), subsequently endorsed by the GA. However, Norway is aware that there are differences of opinion as to where the threshold for breach lies.

[12] *Nicaragua* judgment, para. 202.

[13] *Nicaragua* judgment, para. 205.

example is a cyber operation deliberately causing a temporary shutdown of the target State's critical infrastructure, such as the power supply or TV, radio, Internet or other telecommunications infrastructure in order to compel that State to take a course of action.

## 3.3 Prohibition on the use of force

**Key message:**
**A cyber operation may, depending on its scale and effects, violate the prohibition on the threat or use of force in Article 2(4) of the UN Charter.**

**A cyber operation that is in violation of the prohibition on the threat or use of force may, depending on its scale and effects, constitute an armed attack under international law. An armed attack is the gravest form of the use of force.**

Article 2(4) of the UN Charter prohibits the threat or use of force by a State against the territorial integrity or political independence of another State, or in any other manner inconsistent with the purposes of the UN. The prohibition is a norm of customary international law.[14] It applies to any use of force, regardless of the weapons or means employed.[15]

There are only three exceptions to the prohibition on the use of force in the sense that using force would not be in violation of international law: if the state on whose territory the use of force takes place consents; if it is authorised by the Security Council under Chapter VII of the UN Charter; or in the case of self-defence, in response to an armed attack as recognised in Article 51 of the UN Charter.

Whether a cyber operation violates the prohibition on the threat or use of force in Article 2(4) of the UN Charter depends on its scale and effects, physical or otherwise.[16] Depending on its gravity, a cyber operation may also constitute an armed attack under international law.[17] [18] In accordance with the case law of the International Court of Justice (ICJ), an armed attack is the gravest form of the use of force.[19]

A cyber operation may constitute use of force or even an armed attack if its scale and effects are comparable to those of the use of force or an armed attack by conventional means. This must be determined based on a case-by-case assessment having regard to the specific circumstances. A number of factors may be taken into consideration, such as the severity of the consequences (the level of harm inflicted), immediacy, directness, invasiveness, measurability, military character, State involvement, the nature of the target (such as critical infrastructure) and whether this category of action has generally been characterised as the use of force.[20] This list is not exhaustive.

---

[14] *Nicaragua* judgment, paras. 188-190.

[15] See *Legality of the Threat or Use of Nuclear Weapons*, ICJ, advisory opinion 8 July 1996, para. 39.

[16] *Nicaragua judgment,* para. 195, where ICJ stated that the 'scale and effects' are to be considered when assessing whether particular actions constitute an 'armed attack'. The factors are equally useful and logical when determining whether a cyber operation constitutes the use of force according to Article 2(4) of the UN Charter.

[17] *Nicaragua* judgment, para. 195.

[18] A cyber operation that constitutes an armed attack on a State under international law triggers the right to self-defence under Article 51 of the UN Charter. See *Section 5 Response measures* in this paper.

[19] *Nicaragua* judgment, para. 191: '[. . .] it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'.

[20] Tallinn Manual 2.0., commentary to Rule 69, p. 333-337, paras. 9-10.

Cyber operations that cause death or injury to persons or physical damage to or the destruction of objects could clearly amount to the use of force. Likewise, a cyber operation causing severe disruption to the functioning of the State such as the use of crypto viruses or other forms of digital sabotage against governmental or private power grid- or telecommunications infrastructure, or cyber operations leading to the destruction of stockpiles of Covid-19 vaccines, could amount to the use of force in violation of Article 2(4). Similarly, the use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilisation, may amount to the use of force in violation of Article 2(4).

A cyber operation that severely damages or disables a State's critical infrastructure or functions may furthermore be considered as amounting to an armed attack under international law. Depending on its scale and effect, this may include a cyber operation that causes an aircraft crash.

# 4 State responsibility

**Key message:**
**In order for a State to be held internationally responsible for a cyber operation, the operation has to be attributable to the State under international law.**

**A State may also be held responsible under international law if it possesses knowledge of a cyber operation that is being carried out from its territory and causing serious adverse consequences with respect to a right of the target State under international law, and fails to take reasonably available measures to terminate the cyber operation.**

The general rules on State responsibility under international law apply to cyber operations just as they apply to other activities.

In order for a State to be held responsible for a cyber operation under international law, it is a condition that the cyber operation is attributable to the State under international law.[21] Both State and non-State actors conduct cyber operations. Even if a cyber operation is not conducted by someone acting directly or indirectly on behalf of a State, the State may nevertheless be held responsible under international law if it fails to take adequate measures against cyber operations that target third States from or via its territory.

## 4.1 Attribution under international law

A State may be held responsible under international law for cyber operations conducted by an organ of the State or by actors exercising governmental authority on behalf of the State.[22]

A State may be held responsible under international law for cyber operations conducted by non-State actors if these are conducted on the direct instructions of the State or under its direction or effective control.[23] It may be technically challenging to establish that a relationship between a State and a non-State actor amounts to direct instructions, direction or effective control. However, this is a question of evidence, and not of lack of clarity of international law.

[21] The condition is set out in Article 2 ILC ASR. The other condition, that the act or omission must constitute a breach of an international obligation of the State, is dealt with in Section 3.
[22] Cf. ILC ASR, in particular Articles 4, 5 and 7.
[23] See Article 8 ILC ASR. See also *Nicaragua* judgment, para 115, and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, ICJ, judgment 27 February 2007, para. 400.

## 4.2 Due diligence

Furthermore, a State may be held responsible under international law if it knows or should have known that cyber operations that target third States are being carried out from or via its territory, and fails to take adequate measures.[24]

As a consequence of the right to exercise sovereignty over cyber infrastructure located on its territory, States also have a corresponding obligation not to knowingly allow their territory to be used for acts causing significant harm to the rights of other States under international law. This customary international law obligation, often referred to as the due diligence principle, was recognised by the ICJ in the 1949 *Corfu Channel* judgment,[25] and is reflected in numerous rules in specialised regimes of international law. Norway is of the view that the due diligence obligation applies in situations where there is a risk of transboundary harm from hazardous activities, regardless of the nature of the activity, and accordingly also applies to cyber operations.

Accordingly, if a State possesses knowledge of a cyber operation being carried out from or via its territory causing serious adverse consequences with respect to a right of the target State under international law, it is required to take adequate measures to address the situation.

The due diligence standard is the conduct that is generally considered to be appropriate and proportional to the degree of risk of transboundary harm in the particular instance. It is an obligation of conduct, not of result. Applied to cyber activities, what is required is for the State to take all reasonably available measures to terminate the cyber operation. A breach of the obligation consists not of failing to achieve the desired result, but of failing to take the necessary, diligent steps towards that end. It is irrelevant whether the cyber operation in question is conducted by a third State or a non-State actor. Likewise, it is irrelevant whether the cyber operation in question is conducted by an actor physically present on the State's territory or by an actor making remote use of ICT infrastructure on the State's territory.

In addition to actual knowledge of the use of cyber infrastructure within its territory for harmful cyber operations against another State, a State may also violate its due diligence obligation if it is in fact unaware of the activities in question but objectively should have known about them and fails to address the situation.[26] Accordingly, knowledge also encompasses those situations in which a State in the normal course of events would have become aware that its territory was being used for harmful cyber operations.[27] This implies that the criterion that a State 'should have known' is more likely to be met if for instance the operation used publicly known and easily detected malware, as opposed to highly sophisticated and previously unknown malware.

There is currently no legal basis for a general obligation to prevent cyber operations, and States are consequently not under an obligation to monitor all cyber activities on their territories.[28]

Norway considers the due diligence obligation to be of particular importance in a cyber context. In situations where a targeted State cannot directly attribute (technically and legally) a wrongful cyber operation – for instance election interference – to the State from whose territory it is being carried out, the territorial State may nevertheless still be held accountable on the basis of a breach of the due diligence obligation.

[24] See Article 2 ILC ASR, which explicitly states that a State's conduct may consist of 'an action or omission'. See also *Corfu Channel,* ICJ, judgment 9 April 1949, p. 18.

[25] *Corfu Channel* judgment, 9 April 1949, p. 22

[26] *Corfu Channel* judgment, 9 April 1949, p. 18.

[27] See also Tallinn Manual 2.0, commentary to Rule 6, p. 41.

[28] A general obligation of full control and prevention in the cyber context could be problematic in relation to a State's obligations under international human rights law.

# 5 Response measures

The response measures an injured State may take under international law depend on the severity and nature of the cyber operation and on whether the legally responsible actor behind it is another State or a non-State actor.

## 5.1 Retorsion

A State may respond to any form of cyber operation by retorsion. Retorsion refers to the taking of measures that are lawful but unfriendly, directed against another State. Retorsion may therefore be used regardless of whether international law has been violated and regardless of whether State responsibility applies. Examples of acts of retorsion are breaking off or limiting diplomatic relations, for instance by declaring a diplomat persona non grata, or the imposition of sanctions. Publicly declaring that another State is responsible for a cyber operation is in itself an act of retorsion.

## 5.2 Countermeasures

If a State is the victim of an internationally wrongful cyber operation and another State can be held responsible under customary international law on State responsibility, the injured State may, depending on the circumstances, be entitled to take countermeasures.

A countermeasure is an act that would otherwise be contrary to international law, but where the injured State can invoke the prior internationally wrongful act[29] as a ground for precluding wrongfulness.[30] If there is doubt regarding the attribution of a cyber operation to a State under international law, it may be preferable for the injured State to make use of acts of retorsion rather than countermeasures in order to avoid the possibility of incurring State responsibility for its response.

Countermeasures may only be taken to induce a State to cease an internationally wrongful act or resume its compliance with an international obligation. They are not to be used for punishment and retaliation. Countermeasures must be limited to what is considered necessary and proportional, and may only target the State to which the cyber operation or internationally wrongful act can be attributed. There is no requirement for countermeasures to be of the same nature as the internationally wrongful acts to which they are a response, and countermeasures in response to cyber operations may therefore be carried out within or outside cyberspace. Countermeasures must not violate the prohibition on the threat or use of force or international humanitarian law.

The State held responsible should be notified of both the violation of international law and the grounds for attribution, as well as of the intention to introduce countermeasures.[31] Countermeasures may only be taken if a State has sufficient grounds for attributing the conduct in question to a particular State under international law. What constitutes sufficient grounds will be fact-specific and case-specific, and can be particularly challenging to determine in the case of cyber operations. The State taking countermeasures must be confident in its attribution before resorting to countermeasures. However, the State taking countermeasures need not publish detailed grounds for its attribution or give a detailed technical account of this to the State identified as responsible as this might reveal sensitive methods of interception and detection or offensive and defensive capabilities.

Countermeasures may be taken without prior notification to the responsible State if providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect. For example, the injured State could carry out a cyber operation to disrupt the capability

[29] In this document, 'internationally wrongful acts' must be understood as including both actions and omissions, see Articles 1 and 2 ILC ASR.
[30] See Articles 22 and 49–54 ILC ASR.
[31] ILC ASR Articles 43 and 52.

of the aggressor State conducting the internationally wrongful cyber operation such as election interference. This countermeasure would in other circumstances be in violation of the aggressor State's sovereignty.

### 5.3 Necessity

In a situation of necessity, a State may be able to respond to a cyber operation in a way that is in principle in breach of an international obligation and nevertheless not incur responsibility for its actions under international law.

Necessity refers to those exceptional situations where the only way a State can safeguard an essential interest threatened by a grave and imminent peril, whether cyber in nature or not, is by temporary non-compliance with international obligations of lesser weight or urgency. For instance, if infrastructure in a third country is used in an internationally wrongful cyber operation, the injured State may under certain conditions launch a cyber operation to destroy or disrupt the internationally wrongful cyber operation, even if this violates the territorial sovereignty of the third State.

It is not a requirement that the preceding cyber operation must be attributable to a particular State.

It should be emphasised that, according to customary law on state responsibility, a number of conditions must be fulfilled before necessity can be invoked as a ground for precluding wrongfulness .[32]

### 5.4 Self-defence

A State that is the victim of a cyber operation that qualifies as an armed attack under international law, may exercise its inherent right of individual or collective self-defence under Article 51 of the UN Charter.

The right of self-defence as reflected in Article 51 is a norm of customary international law. It must be exercised subject to the requirements of necessity and proportionality[33], and may involve both digital and conventional means.

## 6 Cyber operations during armed conflicts – international humanitarian law

> **Key message:**
> **International humanitarian law applies to cyber operations in connection with an armed conflict.**

International humanitarian law (IHL) applies in the event of an armed conflict. Whether an (international or non-international) armed conflict exists will depend on the specific circumstances.

This specialised regime of international law, also called *jus in bello*, governs actions, including cyber operations, when they are conducted in connection with an armed conflict.

International humanitarian law aims to minimise the human suffering caused by armed conflict. It thus regulates and limits cyber operations during armed conflicts, just as it regulates and limits the use of any other weapons, means and methods of warfare in an armed conflict.

[32] See Article 25 ILC ASR.
[33] See e.g. *Nicaragua* judgment paras. 176, 194, and *Oil Platforms,* ICJ, judgement 6 November 2003, paras. 43, 73-74, 76.

IHL does not legitimise the use of force in cyberspace. Any use of force by States – either by digital or by conventional means – remains governed by the Charter of the United Nations and the relevant rules of customary international law, also called *jus ad bellum*. Of particular relevance is the prohibition against the use of force. International disputes must be settled by peaceful means, in cyberspace as in all other domains.

The general rules for legitimate military targets are the same regardless of whether conventional or digital means are used. A cyber operation conducted in connection with an armed conflict must be assessed according to its consequences, and may qualify as an attack under international humanitarian law. 'Attack' is a key concept of international humanitarian law, and is understood to mean 'acts of violence against the adversary, whether in offence or defence'.[34] Cyber attacks during armed conflicts are subject to the same restrictions and regulations under international humanitarian law as conventional attacks, including the principles of humanity, military necessity, proportionality and distinction. The concept of attack is particularly relevant to the rules and principles on the selection of targets and precautions. Attacks against civilians or civilian objects are for example prohibited.[35]

Under IHL, medical services must be protected and respected, including when carrying out cyber operations during armed conflict.[36] IHL also prohibits attacking, destroying, removing or rendering useless objects indispensable to the survival of the population, including through cyber means and methods of warfare.[37] 'Objects indispensable to the survival of the civilian population' include ICT infrastructure for food production or drinking water installations.

# 7 Human rights in cyberspace

**Key message:**
**States must comply with their human rights obligations in cyberspace, just as they must in the physical world. States must both respect and protect human rights.**

International human rights law applies to cyber activities just as it does to any other activity. States must comply with their human rights obligations also in cyberspace, as they must in the physical world. States must both respect and protect human rights, including the right to freedom of expression and the right to privacy.

Neither the individuals that are subject to a State's jurisdiction, nor the concept of jurisdiction, is altered by the fact that the activity attributed to the State is a cyber activity. In this respect, cyber activity is no different from other means that States may use to violate their human rights obligations towards their citizens.

[34] Additional Protocol I to the Geneva Conventions of 12 August 1949 relating to the protection of victims of international armed conflict (AP I), Article 49(1).
[35] AP I, Article 51(2) and 52(1).
[36] See, for instance, Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (GCI), Article 19; Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (GCII), Article 12; Convention (IV) relative to the Protection of Civilian Persons in Time of War (GCIV), Article 18; AP I, Article 12; AP II, Article 11; ICRC Customary IHL Study, Rules 25, 28, 29.
[37] AP I, Article 54; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (AP II), Article 14; ICRC Customary IHL Study, Rule 54.