INTERNATIONAL LAW APPLIED TO OPERATIONS IN CYBERSPACE

Paper shared by France with the Open-ended working group established by resolution 75/240

INTRODUCTION

In 2021, the Group of governmental experts (GGE) established pursuant to resolution 73/266, and the Open-ended working group (OEWG) established pursuant to resolution 73/27, reaffirmed in their final reports that "international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment"[1]. Both these reports recommended that States further share views and exchange on how international law applies to cyberspace[2].

France is committed to contributing to these exchanges, in order to continue building common understandings on this issue, to foster transparency and to build confidence regarding State use of ICTs. To that end, this paper[3] summarizes France's views on how international law applies to cyberoperations both in peacetime (Section I) and in situations of armed conflict (Section II). The latter section seeks to clarify in particular how the principles of international humanitarian law (IHL) apply, bearing in mind that "recalling these principles by no means legitimizes or encourages conflict"[4].

[1] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/76/135, 14 July 2021, § 69 ; *Report of the Open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816, 18 March 2021, § 34.

[2] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/76/135, 14 July 2021, § 95b ; *Report of the Open-ended working group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/75/816, 18 March 2021, § 38.

[3] This paper is based on the 2019 document on *International law applied to operations in cyberespace* published by the French Ministry of Armed forces.

[4] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/76/135, 14 July 2021, § 77.

I. CYBEROPERATIONS IN PEACETIME

1.1. France reserves the right to respond to any cyberattack against it that infringes international law

Following on from the positions taken by the GGE[5] and the first OEWG, **France reaffirms the obligation for States to respect international law in cyberspace, including the United Nations Charter, and in particular the principles of the sovereign equality of States, the settlement of international disputes by peaceful means and the requirement for States to refrain in their international relations from the threat or use of force against the integrity or political independence of another State or in any other manner inconsistent with the purposes of the United Nations.**

Many States are acquiring the capacity to prepare and conduct operations in cyberspace. When carried out to the detriment of the rights of other States, such operations may breach international law. Depending on the extent of their intrusion or their effects, they may violate the principles of sovereignty, non-intervention or even the prohibition of the threat or use of force[6]. States targeted by such cyberattacks are entitled to respond to them within the framework of the options offered by international law. In response to a cyberattack, France may consider diplomatic responses to certain incidents, counter-measures, or even coercive action by the armed forces if an attack constitutes armed aggression.

In international law, a cyberoperation is not unlawful *per se* but can become so where it or its effects entail violations of international law.

1.1.1. Cyberattacks may constitute a violation of sovereignty

The international norms and principles that flow from State sovereignty apply to the use of ICT by States and to their territorial jurisdiction over ICT infrastructure[7].

France exercises its sovereignty over the information systems located on its territory[8]. In compliance with the due diligence requirement[9], it ensures that its territory is not used for internationally wrongful acts using ICTs. This is a customary obligation for States, which must (i) use cyberspace in compliance with international law, and in particular not use proxies to commit acts which, using ICTs, infringe the rights of other States, and (ii) ensure that their territory is not used for such purposes, including by non-state actors.

---

[5] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, §§ 25-26.

[6] Article 2, para. 4 of the United Nations Charter: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".

[7] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, §§ 27-28.

[8] Including equipment and infrastructure located on national territory; connected objects, logical components and content operated or processed via electronic communication networks which cover the national territory or from an IP address attributed to France; domains belonging to national registers.

[9] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by the Secretary-General, A/70/174, 22 July 2015, §13 (c).

Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty.

Interference by digital means in the internal or external affairs of France, i.e. interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention.

A cyberattack which penetrates State digital systems, affects the military or economic power, security or survival capacity of the Nation, or constitutes interference in France's internal or external affairs, will entail defensive cyber warfare operations that may include neutralisation of the effect.

The decision whether or not to respond to such operations is a political one, taken in light of the nature and characteristics of the intrusion. The response, chosen from among the range of options offered by international law, depends, subject to an appropriateness assessment, on the gravity of the breach of sovereignty.

The principle of sovereignty applies to cyberspace. France exercises its sovereignty over the information systems located on its territory.

The gravity of a breach of sovereignty will be assessed on a case-by-case basis in accordance with French cyberdefence governance arrangements in order to determine possible responses in compliance with international law.

1.1.2. Some cyberoperations may violate the prohibition of the threat or use of force

The most serious violations of sovereignty, especially those that infringe France's territorial integrity or political independence, may violate the prohibition of the threat or use of force[10], which applies to any use of force, regardless of the weapons employed[11].

In digital space, crossing the threshold of the use of force depends not on the digital means employed but on the effects of the cyberoperation.

A cyberoperation carried out by one State against another State violates the prohibition of the use of force if its effects are similar to those that result from the use of conventional weapons.

However, France does not rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyberoperation may be deemed a use of force against the yardstick of several criteria, including the circumstances prevailing at the time of the operation, such as the origin of the operation and the nature of the instigator (military or not), the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target. This is of course not an exhaustive list. For example, penetrating military systems in order to

[10] "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." There are only three exceptions to the prohibition of the use of force: self-defence in the event of armed aggression (Article 51 of the United Nations Charter), the use of force authorised by the United Nations Security Council under Chapter VII, and the consent of the State on whose territory the operation takes place.

[11] Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, p.18, § 39.

compromise French defence capabilities, or financing or even training individuals to carry out cyberattacks against France, could also be deemed uses of force.

However, **not every use of force is an armed attack within the meaning of Article 51 of the United Nations Charter**[12], especially if its effects are limited or reversible or do not attain a certain level of gravity.

The prohibition of the use of force enshrined in the United Nations Charter applies to cyberspace. Certain cyberoperations may constitute a use of armed force within the meaning of Article 2, para. 4 of the United Nations Charter.

1.1.3. International law authorises several responses to a cyberattack that constitutes a breach of French sovereignty or a use of force

Facing adversaries who make increasing use of cyberattacks, France is taking a number of measures to prevent, anticipate, protect against, detect and respond to them, including by neutralising their effects. For that purpose, the State agencies designated by the Prime Minister are implementing cyberdefence operations designed to anticipate, detect and respond to cyberattacks in coordination with their national and international partners.

In general, France can respond to cyberattacks by taking counter-measures. In response to a cyberattack that infringes international law (including use of force), France may take counter-measures designed to (i) protect its interests and ensure they are respected and (ii) induce the State responsible to comply with its obligations[13].

Under international law, such counter-measures must be taken by France in its capacity as victim. Collective counter-measures are not authorised, which rules out the possibility of France taking such measures in response to an infringement of another State's rights.

Counter-measures must also be taken in compliance with international law[14], in particular the prohibition of the threat or use of force[15]. Consequently, they form part of a peaceful response, their sole purpose being to end the initial violation[16], including in reaction to a cyberoperation that constitutes a use of armed force within the meaning of Article 2, para. 4 of the United Nations Charter. The response to a cyberoperation may involve digital means or not, provided that it is commensurate with the injury suffered, taking into account the gravity of the initial violation and the rights in question[17].

Lastly, the use of counter-measures requires the State responsible for the cyberattack to comply with its obligations. The victim State may, in certain circumstances, derogate from the obligation to inform the State responsible for the cyberoperation beforehand, where there is a need to protect its rights. The possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability.

---

[12] "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."

[13] Article 49, para. 1 of the International Law Commission (ILC) Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[14] Article 50 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[15] Article 50, para. 1(a) of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[16] Article 53 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[17] Article 51 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

In the most serious cases constituting a threat to international peace and security, France may also bring the matter before the UNSC under Chapter VI of the United Nations Charter, or even Chapter VII if there is a threat to peace or breach of peace.

France also does not rule out the option of invoking a state of distress or necessity in order to protect a vital interest against a cyberattack which is below the threshold of armed attack but constitutes a serious and imminent danger. In such cases, the measures taken remain peaceful and do not seriously harm a vital interest of the State concerned.

Such measures in response to a cyberattack against France in breach of international law are not taken systematically, but according to a discretionary political decision.

France has means to prevent, anticipate, protect against, detect and respond to cyberattacks against it in breach of international law. In the event of a cyberattack against its information systems, State agencies may conduct cyberoperations.

On a case-by-case basis, and on a decision by the national cyberdefence chain, such operations may be carried out in the framework of counter-measures.

1.2. A cyberattack that causes damage of a significant scale or severity may constitute an armed attack giving entitlement to the use of self-defence

In accordance with the case law of the International Court of Justice (ICJ), France distinguishes the gravest forms of the use of force, which constitute an armed attack to which the victim State may respond by individual or collective self-defence, from other less grave forms[18]. Cyberattacks may constitute a grave form of the use of force to which France could respond by self-defence.

1.2.1. Categorisation of a cyberattack as an armed attack

France reaffirms that a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter[19], if it is of a scale and severity comparable to those resulting from the use of physical force[20]. In the light of these criteria, the question of whether a cyberattack constitutes armed aggression will be examined on a case-by-case basis having regard to the specific circumstances.

A cyberattack could be categorised as an armed attack if it caused substantial loss of life or considerable physical or economic damage. That would be the case of an operation in cyberspace that caused a failure

[18] ICJ, *Military and Paramilitary activities in and against Nicaragua*, Nicaragua v United States of America, judgment, ICJ Reports 1986, p. 91, § 191: it is necessary "to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms".

[19] As well as in the 2013 *White Paper on Defence and National Security*, this is the position taken in the 2017 *Defence and National Security Strategic Review*: "In cyberspace, certain attacks might be regarded as armed aggression, due to their scale and severity. A major cyberattack may, given the damage it could cause, justify invoking legitimate defence under Article 51 of the UN Charter" (§ 90), and in the 2018 *Strategic Review of Cyberdefence*: "A major cyberattack on France, in view of the serious damage it would cause, could constitute an 'armed attack' within the meaning of Article 51 of the United Nations Charter and justify invoking self-defence" (p. 82).

[20] *Military and Paramilitary activities in and against Nicaragua*, Nicaragua v United States of America, judgment, ICJ Reports 1986, p. 93, § 195. Article 2 of UNGA Resolution 3314 (1974): "The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression", provided that "the acts concerned or their consequences are […] of sufficient gravity".

of critical infrastructure[21] with significant consequences or consequences liable to paralyse whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims[22]. In such an event, the effects of the operation would be similar to those that would result from the use of conventional weapons[23].

To be categorised as an armed attack, a cyberattack must also have been perpetrated, directly or indirectly, by a State. Leaving aside acts perpetrated by persons belonging to State organs or exercising elements of governmental authority, a State is responsible for acts perpetrated by non-state actors only if they act de facto on its instructions or orders or under its control in accordance with the rules on State responsibility for internationally wrongful acts and ICJ case law.

In accordance with ICJ case law, France does not recognise the extension of the right to self-defence to acts perpetrated by non-state actors whose actions are not attributable, directly or indirectly, to a State.

France has, in exceptional cases, invoked self-defence against an armed attack perpetrated by an actor having the characteristics of a "quasi-State", as with its intervention in Syria against the terrorist group Daesh (ISIS/ISIL)[24]. However, this exceptional case cannot constitute the definitive expression of recognition of the extension of the concept of self-defence to acts perpetrated by non-state actors acting without the direct or indirect support of a State.

Nonetheless, it cannot be ruled out that general practice may shift towards an interpretation of the law of self-defence as being authorised in response to an armed attack by non-state actors whose acts are not attributable to a State. However, any such development will have to be made bearing in mind the Rome Statute of the International Criminal Court (ICC) as amended in 2010 to add the crime of aggression[25], and the case law of the ICC that may emerge in this sphere[26].

1.2.2. Use of the right of self-defence against a digital armed attack

Under Article 51 of the United Nations Charter, a State that suffers an armed attack is entitled to use individual or collective self-defence. Self-defence in response to an armed attack carried out in cyberspace may involve digital or conventional means in compliance with the principles of necessity

[21] SGDSN, *Strategic Review of Cyberdefence*, 2018, p. 61.
[22] *White Paper on Defence and National Security*, 2013, p. 48.
[23] *White Paper on Defence and National Security*, 2013, p. 48.
[24] France based the lawful nature of its intervention against Daech in Syria firstly on the principle of collective self-defence in favour of Iraq, then, after the attacks of 13 November 2015, on the basis of individual self-defence.
[25] Article 8bis of the Rome Statute defines the crime of aggression as an act perpetrated by "a person in a position effectively to exercise control over or to direct the political or military action of a State which, by its character, gravity and scale" – hence regardless of the means employed – "constitutes a manifest violation of the Charter of the United Nations".
[26] The ICC has had jurisdiction over the crime of aggression since July 2018.

and proportionality[27]. On a decision by the President of the Republic to commit the French armed forces, the Armed Forces Ministry may carry out cyberoperations[28] for military purposes in cyberspace.

Cyberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity[29], or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert.

In exceptional circumstances, France allows itself to use pre-emptive self-defence in response to a cyberattack that "has not yet been triggered but is about to be, in an imminent and certain manner, provided that the potential impact of such an attack is sufficiently serious"[30]. **However, it does not recognise the legality of the use of force on the grounds of preventive self-defence[31].**

States which, in the conduct of a cyberoperation or in their response to a cyberattack, decide to use non-state actors, such as companies providing offensive cyber services or groups of hackers, are responsible for those actors' actions. In view of the risk of systemic instability arising from the private-sector use of offensive capabilities, France, following on from the Paris Call, is in favour of regulating them strictly and prohibiting such non-state actors from carrying out offensive activities in cyberspace for themselves or on behalf of other non-state actors[32].

Lastly, any response on the grounds of self-defence remains provisional and subordinate. It must be promptly reported to the UNSC[33] and suspended as soon as the Security Council takes the matter in hand, replacing unilateral action with collective measures or, failing that, as soon as it has achieved its purpose, namely to repel or end the armed attack. Other measures, such as counter-measures or referral to the UNSC, may be preferred if they are deemed more appropriate.

The specific characteristics of cyberspace do not call into question France's position with regard to self-defence in response to cyberattacks which reach the threshold of an armed attack within the meaning of Article 51 of the United Nations Charter.

In response to an armed attack carried out via a digital vector, the use of force by digital or conventional means must meet the criteria of necessity and proportionality.

---

[27] "The Parties also agree in holding that whether the response to the attack is lawful depends on observance of the criteria of the necessity and the proportionality of the measures taken in self-defence. […] The measures must not merely be such as to tend to protect the essential security interests of the party taking them, but must be 'necessary' for that purpose", *Military and Paramilitary activities in and against Nicaragua*, Nicaragua v United States of America, judgment, ICJ Reports 1986, §194 and §282. "There is a specific rule […] well established in customary international law" whereby "self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it", Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, § 41.

[28] More specifically, offensive cyber warfare operations.

[29] SGDSN, *Strategic Review of Cyberdefence*, 2018, p. 82. In the Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), the ICJ does not rule out the approach consisting in assessing whether a series of attacks against the United States can be categorised as an armed attack (Judgment, ICJ Reports, 2003, § 64).

[30] SGDSN, *Strategic Review of Cyberdefence*, 2018, p. 84.

[31] Preventive self-defence is exercised in response to a potential armed attack, i.e. one that is latent and more or less likely to occur in the future.

[32] SGDSN, *Strategic Review of Cyberdefence*, 2018, p.88.

[33] Article 51 of the United Nations Charter: "Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council".

1.2.3. The failure by another State to comply with its due diligence requirement is not a sufficient ground for the use of force against it in the context of cyberattacks carried out from its territory

In accordance with the due diligence principle, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs"[34], including acts that infringe the territorial integrity or sovereignty of another State[35]. In addition, States must ensure that non-state actors do not use their territory to carry on such activities, and not use proxies to commit internationally wrongful acts using ICTs[36]. The fact that a State fails to comply with its due diligence obligation can justify the taking of political and diplomatic measures[37] that may include counter-measures or a referral to the UNSC.

The fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-state actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force[38].

Under these conditions, France does not recognise the extensive approach to self-defence expressed by a majority of the Tallinn Manual Group of Experts[39] which allows a State that is victim of a large-scale cyberattack perpetrated by non-state actors from the territory of another State to use self-defence against that State, including if such a response is carried out in compliance with the principle of necessity, is the only means to counter the armed attack, and the territorial State is unwilling or unable to prevent the perpetration of such acts.

Under the due diligence obligation, States should ensure that their sovereign domain in cyberspace is not used to commit internationally unlawful acts.

A State's failure to comply with this obligation is not a ground for an exception to the prohibition of the use of force.

1.3. The attribution of a cyberattack having its origin in another State is a national political decision

The cyberattacks confronting States and private-sector actors are by nature difficult to characterise in cyberspace. Digital resources are used for the purposes of espionage, cyber crime, destabilisation and even sabotage. The inherent characteristics of this environment, the difficulty of

[34] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by the Secretary-General, A/70/174, 22 July 2015, §13 (c).

[35] Case Concerning United States Diplomatic and Consular Staff in Tehran, United States of America v. Iran, judgment, ICJ Reports 1980, §§ 61-8.

[36] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, Note by the Secretary-General, A/70/174, 22 July 2015, § 28.

[37] SGDSN, *Strategic Review of Cyberdefence*, 2018, Annex 7 on options in response to cyberattacks, p. 159.

[38] There are only three exceptions to the prohibition of the use of force: self-defence against an armed attack (Article 51 of the United Nations Charter), the use of force authorised by the UNSC under Chapter VII, and the consent of the State on whose territory the intervention occurs.

[39] "Self-defence against a cyber armed attack (…) is permissible when it complies with the principle of necessity (Rule 72), is the only effective means of defence against the armed attack, and the territorial State is unable (e.g. because its lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack. In particular, these Experts emphasised that States have a duty to ensure their territory is not used for acts contrary to international law (Rule 6)", Michael Schmitt and Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press*, 2017, Rule 71, p. 339.

tracing and controlling activities, the increasingly extensive involvement of non-state actors and the possibilities available to States of using private-sector actors as proxies to carry out malicious activities make the identification of the perpetrators and sponsors of such attacks a particularly complex affair.

When a cyberattack is detected, France takes the necessary steps to categorise it, which may include neutralising its effects. Identification of the instigator is based mainly, though not solely, on technical information gathered during investigations of the cyberattack, especially identification of the attack and transit infrastructure for the cyberoperation and its location, identification of the adversary methods of operation (AMO), the overall chronology of the perpetrator's activities, the scale and gravity of the incident and the compromised perimeter, or the effects sought by the attacker[40]. This information can help to determine whether or not a link exists between the instigators and a State.

A cyberattack is deemed to have been instigated by a State if it has been perpetrated by a State organ[41], a person or entity exercising elements of governmental authority[42], or a person or group of persons acting on the instructions of, or under the direction or control of that State[43].

The identification of a State as being responsible for a cyberattack that is an internationally unlawful act does not in any way oblige the victim State to make a public attribution. Such attribution is a discretionary choice made, inter alia, according to the nature and origin of the operation, the specific circumstances and the international context. It is a sovereign decision insofar as **France reserves the right to attribute publicly, or not, a cyberattack against it and to bring that information to the attention of its population, other States or the international community.** This policy does not rule out close coordination with France's allies and partner States, including international or regional organisations, in particular the European Union (EU) and the North Atlantic Treaty Organisation (NATO). However, while the decision may go as far as collective attribution of a cyberattack, it lies solely with France. In addition, international law does not require States to provide the evidence on which the public attribution of a cyberattack is based, though such information helps to legitimise the validity of such attribution.

In all events, a decision not to publicly attribute a cyberattack is not a final barrier to the application of international law, and in particular to assertion of the right of response available to States[44].

The public attribution of a cyberattack against France is a national political decision. Although this power may be exercised in coordination with other States or international organisations, it is *prima facie* a sovereign prerogative.

[40] Armed Forces Ministry Instruction n. 101000/ARM/CAB of 7 February 2019 on defensive cyber warfare policy.

[41] Article 4, para. 1 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[42] Article 5 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[43] Article 8 of the ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts.

[44] "Non-attribution is not a final barrier to the application of existing international law, especially as neutral means of action are available under international law", SGDSN, *Strategic Review of Cyber Defence*, 2018, p. 82.

II. INTERNATIONAL LAW APPLICABLE TO CYBEROPERATIONS IN ARMED CONFLICT SITUATIONS

In an armed conflict situation, cyberspace is an area of confrontation in its own right in the same way as land, sea, air and outer space[45].

In response to this new form of conflict, the Armed Forces Ministry fully integrates the cyber dimension into its military operations. Although offensive cyber warfare is a strategic capability, it is also a tactical weapon whose effects can be combined with those of conventional weapons.

The complexity involved in using a cyber weapon means that it is necessary to control all its effects within a framework that complies with IHL. Offensive cyber warfare resources are used by the French armed forces only in compliance with the principles governing the conduct of hostilities, in the same way as operations planned and carried out exclusively in the physical domain.

2.1. Cyberoperations may characterise the existence of armed conflict

Cyberoperations that constitute hostilities between two or more States may characterise the existence of international armed conflict (IAC)[46]. Likewise, prolonged cyberoperations by government armed forces against one or more armed groups or by several armed groups between themselves may constitute a non-international armed conflict (NIAC), where such groups show a minimum level of organisation and the effects of such operations reach a sufficient threshold of violence[47].

They are generally military operations concurrent with conventional military operations: that is why it is not difficult to categorise an armed conflict situation. While an armed conflict consisting exclusively of digital activities cannot be ruled out in principle, it is based on the capacity of autonomous cyberoperations to reach the threshold of violence required to be categorised as such.

Although virtual, cyberoperations still fall within the geographical scope of IHL, insofar as their effects must arise on the territory of the States party to the IAC and on the territory where the NIAC hostilities occur.

---

[45] *White Paper on Defence and National Security*, 2013: "information systems are now part and parcel of our societies". The 2017 Defence and National Security Strategic Review states that digital space "has become a real domain of confrontation and is the subject of intense strategic competition".

[46] Common Article 2 to the Geneva Conventions (1949) and Article 1, para. 3 of AP I.

[47] In the case of a prolonged armed confrontation reaching a certain level of intensity between two parties including at least one non-state party, IHL distinguishes between low-intensity NIACs governed by Common Article 3 to the Geneva Conventions (the armed group or groups show a minimum level of organisation) and high-intensity NIACs governed by Common Article 3 and Additional Protocol II (AP II) (the level of organisation required of the armed group or groups is particularly high: responsible command, exercise of control over part of the territory such that sustained and concerted military operations can be conducted). A NIAC may be exported where the parties to an initial NIAC extend their hostilities into the territory of one or more neighbouring States with the consent of the State or States concerned. The criteria applicable to the exported NIAC are the same as those applicable to the original NIAC (identity of the parties and intensity of the violence). Thus, operations in cyberspace, in isolation or linked with conventional operations, which fulfil these criteria may constitute an exported NIAC.

Cyberoperations dedicated to the engagement of armed forces in an armed conflict situation are governed by IHL.

A cyberoperation that constitutes a confrontation between States may characterise the existence of an IAC. The state of technology seems for the time being to rule out the possibility of cyberoperations alone reaching the necessary threshold of violence to characterise a NIAC situation.

Cyber resources are first and foremost used in combination with and to support conventional effects. Although cyberspace is virtual, these operations are still subject to the geographical scope of the conflict in which they are conducted.

2.2. IHL applies to all cyberoperations carried out in, and in connection with, an armed conflict situation

The use of a cyber weapon in an armed conflict situation obeys the principles governing the conduct of hostilities. A cyber weapon, which is governed by IHL, may be used in combination with conventional military resources or in isolation. In support of conventional means, it produces the same intelligence, neutralisation and deception effects as those conventional means, which have long been subject to the targeting procedures used by the French armed forces in compliance with IHL.

The specific nature and complexity of offensive cyber warfare resources demand risk control arrangements just as robust as those applied to conventional operations, taking into account the inherent features of the conduct of operations in cyberspace. In practice, the risks linked to the use of a cyber weapon, especially the immediacy of the action, the duality of targets and the hyperconnectivity of networks, demand a specific digital targeting process spanning all phases of the cyberoperation in order to ensure compliance with the principles of distinction, precaution and proportionality, inter alia in order to minimise potential civilian damage and loss of life. The process involves long and specific planning carried out in close coordination with the planning of operations in the physical sphere.

2.2.1. A cyberoperation may constitute an attack within the meaning of international humanitarian law

Any cyberoperation which is carried out in, and in connection with, an armed conflict situation, and constitutes an act of violence, whether offensive or defensive, against another party to the conflict, is an attack within the meaning of Article 49 of AP I to the Geneva Conventions[48].

In an armed conflict situation, the primary purpose of cyber weapons is to produce effects against an adversary system in order to alter the availability, integrity or confidentiality of data. Their effects may be material (e.g. neutralisation of a weapons system) or virtual (e.g. intelligence gathering), temporary, reversible or final[49].

For example, the destruction of adversary military offensive cyber or conventional capabilities by disruption or the creation of major damage is an attack within the meaning of IHL. The same applies to neutralisation actions which damage adversary cyber or conventional military capabilities by destroying ICT equipment or systems or altering or deleting digital data or flows such as to disable a service essential to the operation of such capabilities.

[48] Article 49 of AP I: "'Attacks' means acts of violence against the adversary, whether in offence or in defence".
[49] Public Elements for the Military Cyber Warfare Doctrine, 2019.

Contrary to the definition given by the Tallinn Manual Group of Experts[50], France does not characterise a cyberattack solely on the basis of material criteria. It considers that a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterised where action by the adversary is necessary to restore the infrastructure or system (repair of equipment, replacement of a part, reinstallation of a network, etc.).

Most cyberoperations carried out by the French armed forces in an armed conflict situation (mainly information-gathering) do not meet the definition of an attack. For example, altering the adversary's propaganda capabilities, and in particular making an influence site unavailable by saturation or denial of service – which is not prohibited by IHL by analogy with conventional jamming of radio communications or TV broadcasts – cannot be characterised as an attack. However, such operations, in the same way as general information-gathering with the aim of evaluating the adversary's military capabilities or hacking a system in order to gather data, are still governed by the provisions of IHL applicable to any military operation carried out in an armed conflict situation.

France considers that an attack within the meaning of Article 49 of AP I may occur even if there is no human injury or loss of life, or physical damage to goods. Thus, a cyberoperation constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required in order to restore the infrastructure or the system.

Most cyberoperations, including offensive cyber warfare operations carried out by France in an armed conflict situation, remain below the attack threshold, since they mostly involve information-gathering and the jamming of the adversary's influence capabilities. Such operations remain nonetheless governed by the general principles of IHL.

2.2.2. Application of the principles governing the conduct of hostilities

In a military environment characterised by (i) the changing risk of conflict, (ii) the lack of a clearly defined front line and (iii) the involvement of adversaries who blend in with the civilian population and use various and asymmetrical methods of action, applying the rules governing the conduct of hostilities is a particularly complex business. That complexity is exacerbated in cyberspace, where the immediacy of action, the duality of targets and the hyperconnectivity of information systems and networks mean that the effects of a cyberoperation are lightning fast.

In order to ensure application of the rules governing the conduct of hostilities (distinction, proportionality and precaution, prohibition of superfluous injury and unnecessary suffering[51]), a specific digital targeting process is used for cyberoperations, under the responsibility of the commander-in-chief

[50] "Definition of cyberattack. A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects", Michael Schmitt and Liis Vihul (dir.), The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Rule 92, p. 415.

[51] This principle prohibits causing injury and suffering, not only to civilians but also to combatants and members of organised armed groups, insofar as they are not necessary to achieve strictly military objectives. In this regard, the use of weapons, projectiles and materials and methods of warfare likely to cause such suffering, whether physical or moral, is prohibited. As far as operations carried out by France in cyberspace are concerned (against digital infrastructure and systems), the principle is taken into account but has no practical application and will consequently not be analysed as such.

of the armed forces, with the input, inter alia, of operational staff and specialist operational legal advisers.

It cannot be ruled out that a serious breach of these principles arising from a cyberoperation could constitute a war crime within the meaning of the Rome Statute[52].

• <u>The principle of distinction</u>

Under the principle of distinction, the parties to an armed conflict must at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives[53]. In this regard, cyber-attacks carried out in an armed conflict situation which are not directed against a specific military objective or whose effects cannot be contained are prohibited[54]. If there is doubt as to whether an individual is a combatant, he or she must be considered a civilian[55]. Likewise, an object normally used for civilian purposes is presumed not to be used to make an effective contribution to military action[56]. On this point France does not follow the Tallinn Manual[57], which considers that if there is doubt over the use of a civilian object for military purposes, a determination as to such use should be made only following a careful assessment.

From this standpoint and under the authority of the commander-in-chief of the armed forces, offensive cyber warfare operations are planned and coordinated taking all measures possible in practice to ensure that the targeted objectives are not civilians or civilian objects. Commanders are thus careful to gather the necessary intelligence to identify the objective and choose the most suitable means in order to apply the principle of distinction. Even if cyber weapons can have immediate effects, their integration into the operational manoeuvre is based on often long and specific planning designed to gather the information necessary to identify the nature of the targeted system (such as a map of the enemy network) in order to ensure compliance with IHL. A cyberoperation will be cancelled if the target under consideration proves not to be a military objective.

− <u>The distinction between military objectives and civilian objects[58]</u>

In cyberspace, ICT equipment or systems and the data, processes or flows which constitute a service may be a military objective if (i) they contribute to military action by their nature (armed forces computer workstations, military command, localisation or surveillance networks, etc.), their location (places from which the cyber-attacks are carried out), their purpose (foreseeable use of ICT networks for military purposes) or their use (use of part of the network for military purposes), and (ii) their total or partial destruction, capture or neutralisation confers a definite military advantage. Under these circumstances,

[52] Michael Schmitt and Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rules 84-85, pp. 391-400.
[53] Article 48 of AP I: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives".
[54] Article 51, para. 4 of AP I.
[55] Articles 50, para. 3 and 52, para. 3 of AP I.
[56] Article 52, para. 3 of AP I.
[57] "In case of doubt as to whether an object and associated cyber infrastructure that is normally dedicated to civilian purposes is being used to make an effective contribution to military action, a determination that it is so being used may only be made following a careful assessment", Michael Schmitt and Liis Vihul (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, Rule 102, p. 448.
[58] Article 52, para. 2 of AP I.

a propaganda centre may be a lawful military objective and the target of a cyberattack if it disseminates instructions linked to the conduct of hostilities[59].

Conversely, all objects which are not military objectives are deemed to be civilian objects[60]. An attack carried out in cyberspace may not be directed against ICT systems used by schools, medical institutions or any other exclusively civilian service, or against systems whose destruction would only entail tangible effects on civilian objects, unless those objects are used for military purposes. Given the current state of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction.

Cyberoperations must also take into account the special protection of certain objects, such as medical units[61], cultural property[62], the natural environment[63], objects indispensable to the survival of the civilian population[64] and installations that contain dangerous forces[65]. This protection extends to ICT equipment and services and to the data needed to operate them, such as medical data linked to the operation of a hospital.

ICT infrastructure or a system used for both civilian and military purposes may, after detailed analysis on a case-by-case basis, be deemed a military objective. They may be targeted provided that the principles of proportionality and precaution are respected. Given the hyperconnectivity of systems, commanders exercise vigilance over the action as a whole in order to avoid effects on civilians and civilian objects, or at least keep them to a minimum, in compliance with the principles of precaution and proportionality.

− **The distinction between civilians and combatants[66]**

Cyber-combatants[67], especially military personnel assigned to a cyberspace operations command, a group of hackers under State command or members of organised armed groups[68] perpetrating cyberoperations against the adversary may be attacked, unless they are hors de combat.

[59] International Criminal Tribunal for Rwanda (TPIR), The Prosecutor v. Nahimana, Barayagwiza and Ngeze, 3 December 2013, ICTR-99-52-T, Judgment. This was the case of the Radio des Milles Collines in Rwanda, which broadcast specific information about the location of Tutsis and gave them false information to encourage them to gather in supposedly protected areas.

[60] Article 52, para. 1 of AP I.

[61] Articles 19.1, 24, 25, 35 and 36 of the First Geneva Convention (1949); Articles 22, para. 1, 36 and 39 of the Second Geneva Convention (1946); Articles 18, para. 1, 20, para. 1 and 22, para. 1 of the Fourth Geneva Convention (1949); Articles 12.1, 15.1 and 21 of AP I.

[62] Article 53 of AP I and Convention for the Protection of Cultural Property in the Event of Armed Conflict, 1954.

[63] Article 35, para. 3 and 55, para. 1 of AP I.

[64] Articles 54, para. 2 of API and 14 of AP II.

[65] Article 56, para. 2 of AP I.

[66] Article 48 of AP I.

[67] Article 43 of AP I.

[68] The International Criminal Tribunal for the former Yugoslavia (ICTY) listed a number of criteria on the basis of which an armed group could be deemed "organised", including the existence of a command structure and disciplinary rules and mechanisms within the group, the existence of headquarters, the group's control of a certain amount of territory, its ability to procure weapons, other military equipment and recruits and provide military training, its capacity to plan, coordinate and carry out military operations, including troop movements and logistical operations, its ability to determine a unified military strategy and to conduct large-scale military operations, and its capacity to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords. For more information on the level of organisation required, see esp. ICTY, The Prosecutor v. Boškoski and Tarculovski, ICTY-IT–04–82-T, Judgment of the Chamber of First Instance of 10 July 2008, §§ 194-205.

Any other person is considered to be a civilian and enjoys general protection against the dangers arising from military operations[69], unless and for such time as they take a direct part in hostilities[70]. A cyberoperation which is carried out to adversely affect the military operations or military capacity of a party to an armed conflict to the detriment of that party and to the advantage of an adversary, or which is likely to cause loss of human life, injury and civilian damage may be deemed a direct participation in hostilities[71].

For example, the penetration of a military system by a party to an armed conflict with a view to gathering tactical intelligence for the benefit of an adversary for the purposes of an attack constitutes direct participation in hostilities. The same applies to installing malicious code, preparing a botnet in order to launch an attack by denial of service, or developing software specifically intended for the perpetration of a hostile act[72].

In the conduct of cyber warfare operations, the essential aim of the digital targeting process is to comply with the military objective criterion in terms of distinction, given the nature of the targets (digital systems and infrastructure).

France interprets Article 52, para. 3 of AP I as requiring States, in case of doubt, to presume the civilian nature of an object normally dedicated to civilian purposes and not as requiring a new determination in order to decide whether or not it makes an effective contribution to military action.

Although intangible, France considers that civilian content data may be deemed protected objects. The special protection afforded to certain objects extends to systems and the data that enable them to operate.

Cyber-combatants integrated into or affiliated with the armed forces or members of organised armed groups may be targeted by conventional means, in the same way as civilians conducting offensive activities that constitute direct participation in hostilities. Given the difficulties of identifying the perpetrators of a cyberattack, the targeting of such individuals remains marginal.

• **<u>The principles of proportionality and precaution</u>**

When cyberoperations are conducted, constant care should be taken to spare the civilian population, civilians and civilian objects[73].

Even though the necessary precautions may be taken, if the neutralisation or destruction of a military objective by digital means nevertheless risks causing civilian damage, it must not exceed the concrete and direct military advantage anticipated[74]. The risks inherent in cyberspace (immediacy of effects, intrinsic duality of military objectives, hyperconnectivity, difficulty of tracing operations, vulnerability of systems) must therefore be taken into account in order to determine the modes of action and means to be implemented in cyber warfare in order to ensure compliance with the principle of proportionality.

[69] Article 51, para. 1 of AP I.
[70] Article 51, para. 3 of AP I and Article 13 of AP II.
[71] The criteria of threshold of harm, direct causation and belligerent nexus must be fulfilled.
[72] The above-mentioned criteria must be fulfilled.
[73] Article 57, para. 1 of AP I.
[74] Article 57, para. 2(a)(iii) of AP I.

Even though the anticipated effect of a cyber weapon may be difficult to measure, given the interconnectivity of information systems, especially on account of the risk of propagation beyond the target, these risks may be contained by the development of specific cyber weapons whose use is decided according to the desired effects, determined beforehand (activation of malware only in the presence of a specific network previously identified by a penetration of the system, existence of a deactivation time, etc.).

The use of malware which deliberately reproduces and propagates with no possible control or reversibility, and is hence likely to cause significant damage to critical civilian systems or infrastructure, is contrary to IHL, in the same way as the temporary interruption without military advantage of an adversary system followed by physical damage to civilian infrastructure.

The assessment of the effects of a cyberoperation takes into account all the foreseeable damage caused by the cyber weapon, whether direct (such as damage to the ICT equipment directly targeted or interruption of the system) or indirect (such as the effects on the infrastructure controlled by the targeted system, or on persons affected by the malfunction or destruction of the targeted systems or infrastructure, or by the alteration and corruption of content data).

In order for offensive cyber warfare operations to be conducted in compliance with the principle of precaution, the Armed Forces Ministry consults operational experts in military cyberdefence under the responsibility of the cyberdefence commander (COMCYBER). They possess the necessary technical knowledge, are able to exploit the available information (intelligence, strict identification of targets, correlation between the weapon and the desired effects, etc.) and have been given specific training in the complexity of cyber weapons.

These precautionary measures in attack are backed up by precautionary measures against the effects of an attack which a State should take in order to protect the civilian population and civilian objects against the dangers resulting from cyberoperations[75].

Despite the complexity of cyberspace, the framework for cyberoperations carried out in an armed conflict situation is still determined by compliance with the principles of precaution and proportionality. As such, the digital targeting process takes account of a cyber weapon's direct and indirect effects.

Despite the interconnectivity of military and civilian systems, the fact of being able to configure a cyber weapon according to the specifically desired effects of an operation helps to avoid excessive damage in relation to the concrete and direct military advantage anticipated. The non-lethal nature of cyber weapons and the possibility of limiting their effects to a previously identified system contribute to the obligation to choose the means and methods of attack most likely to avoid, or at least reduce to a minimum, any incidental loss of civilian lives, injury to civilians or damage to civilian objects.

2.3. <u>The law of neutrality applies in cyberspace</u>

Cyberoperations carried out in the context of an international armed conflict, or which trigger such a conflict, are subject to the law of neutrality[76]. As such, the States party to an IAC may neither carry out

[75] Article 58 of AP I.

[76] "[A]s in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the relevant provisions of the United Nations

cyberoperations linked to the conflict from installations situated on the territory of a neutral State or under the exclusive control of a neutral State, nor take control of computer systems of the neutral State in order to carry out such operations[77]. The neutral State must prevent any use by belligerent States of ICT infrastructure situated on its territory or under its exclusive control. However, it is not required to prevent belligerent States from using its ICT networks for communication purposes[78].

Routing a cyberattack via the systems of a neutral State without any effect on that State does not breach the law of neutrality, which prohibits only the physical transit of troops or convoys.

The law of neutrality applies to cyberoperations. Belligerents must refrain from causing harmful effects to digital infrastructure situated on the territory of a neutral State or from launching a cyberattack from such infrastructure.

Charter) to all international armed conflict, whatever type of weapons might be used", Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, p. 39, § 89.

[77] Article 1 of Convention V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, and of Convention XIII respecting the Rights and Duties of Neutral Powers in Naval War, The Hague, 18 October 1907.

[78] Article 8 of Convention V respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907.

GLOSSARY

Cyber weapon

Digital capability(ies), including digital warfare weapons, resources and methods, used in a cyberoperation against the adversary in and in connection with an armed conflict situation.

Cyberattack

A deliberate offensive or malicious action carried out via cyberspace and intended to cause damage (in terms of availability, integrity or confidentiality) to data or the systems that treat them, which may consequently harm the activities for which they are the medium. A cyberattack may be a cyberoperation carried out by a State against the interests of the French State.

Cyberdefence

The set of technical and non-technical measures taken by a State to defend in cyberspace information systems deemed of vital importance which help to ensure cyber security.

Military cyberdefence

A coordinated set of defensive and offensive actions carried out in cyberspace during the planning, preparation or conduct of military operations. It is based on six major missions: prevent, anticipate, protect, detect, respond and attribute.

Cyberspace

The communication space formed by the global interconnection of automated digital data processing infrastructure and equipment and by the objects connected to it and the data processed in it.

Cyberoperations

Defensive or offensive cyber warfare or cyberintelligence actions.

Cybersecurity

A state sought for an information system in which it can resist events emanating from cyberspace such as to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and the related services which such systems offer or to which they give access. Cybersecurity makes use of information systems security techniques and is backed up by the fight against cybercrime and the implementation of cyberdefence.

Critical infrastructure

Infrastructure that provides goods and services essential to the Nation, or breaches of whose availability, integrity or confidentiality may present a grave danger, in particular for the population.

Defensive cyber warfare

A coordinated set of actions carried out by a State which consists in detecting, analysing and preventing cyber-attacks and responding to them where appropriate.

Offensive cyber warfare

A set of actions carried out in cyberspace producing effects against an adversary system in order to alter the availability or confidentiality of data.