Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Directorate of International Law DIL

Switzerland's position paper on the application of international law in cyberspace

Annex UN GGE 2019/2021

Introduction

In the context of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2019/2021 (UN GGE), the primary focus of states lies on the security-related aspects in the digital space (cybersecurity) and the applicable provisions under international law in this area.[1] The use of the term 'cyberspace' in the present position paper therefore refers only to that part of the digital space which concerns the security dimension. Part I addresses questions concerning international law in general including human rights. Part II places particular emphasis on questions relating to international humanitarian law (IHL).

Switzerland is committed to building and maintaining a free, open, secure and peaceful cyberspace, and to advancing the recognition, observance and enforcement of international law in this space.[2] All states have a common interest in ensuring that cyberspace is governed by the rule of law and used for peaceful purposes only. Switzerland considers international law to be applicable to cyberspace. It therefore welcomes the consensus of previous UN GGEs that international law, and in particular the UN Charter in its entirety, are applicable to cyberspace[3] – which was also approved unanimously by the UN General Assembly.[4] It also welcomes the OEWG 2019/2021 report of 18 March 2021, which confirms this consensus.[5]

Switzerland views national positions of states as an important contribution to fleshing out the application of international law in cyberspace. This paper therefore gives an overview of Switzerland's position, but is neither exhaustive nor conclusive. Continuing intergovernmental

---

1 On Switzerland's work to establish an international regulatory framework in the digital space in general, refer to the Digital Foreign Policy Strategy (2021–24) and Annex 4 on the international rules and standards in particular (https://www.eda.admin.ch/dam/eda/en/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_EN.pdf).

2 See Switzerland's Foreign Policy Strategy 2021–23, Objective 4.4 and Switzerland's Digital Foreign Policy Strategy 2021–24, Chapter 4.3.

3 See Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013 Report (2013 Report, UN Doc. A/68/98, para. 19; 2015 Report (UN Doc. A/70/174), para. 24, para. 28 c).

4 Resolution A/70/237.

5 See Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021 report, para. 8, UN Doc. A/75/816.

exchange at multilateral level remains key in order to continue to clarify how international law is applicable to cyberspace in concrete terms. A definitive assessment of a cyber incident in terms of international law is only possible when the concrete circumstances are known. This means interpreting and applying the rules set out below in each individual case.

Of particular importance to the context of cybersecurity are namely the rules of international law described below.

I. General international law

1. Peaceful settlement of disputes

In accordance with Art. 2 para. 3 and Art. 33 of the UN Charter, disputes which may endanger the maintenance of international peace and security should be settled by peaceful means. This includes diplomatic proceedings, arbitration or recourse to the International Court of Justice (ICJ). As a neutral country with long-standing experience and engagement in the provision of good offices, Switzerland is committed to upholding this principle in cyberspace, emphasising the overriding aim of ensuring that cyberspace is used for peaceful purposes only. Switzerland therefore welcomes the UN GGE's 2015 report and the OEWG 2019/2021 report confirming the peaceful settlement of disputes as one of the UN Charter's central principles, which is also applicable to cyberspace. Consequently, disputes in cyberspace should also be settled by peaceful means, not with unilateral measures.

2. Sovereignty

Sovereignty is a foundational principle of international law. It refers to a state's jurisdiction to define, apply and enforce its own legal order, which in principle is limited to its territory. At interstate level however, sovereignty implies an independent and equal co-existence among states. Respect for and protection from interference with territorial integrity is a product of state sovereignty.[6] Accordingly, each state is obliged to respect the sovereignty of other states.[7] Sovereignty is a binding primary rule of international law. Violations of sovereignty are therefore considered internationally wrongful acts which, if attributable to the state itself, give rise to state responsibility.

State sovereignty is also applicable to cyberspace.[8] Owing to the special characteristics of cyberspace, which has no clear territorial boundaries, putting the principle of sovereignty into practice is a particular challenge. One major issue is who has jurisdiction over or access to digital data. In the cyber context, the key question is which states have legitimate control over digital data and are authorised to access that data – which may, depending on the circumstances, be stored on a different territory or may not be localised geographically. Conversely, in terms of interstate relations at cybersecurity level, the principle of sovereignty provides wide scope for protection against cyber operations. For example, state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised intrusion or material damage. This includes the computer networks,

---

6 Arbitration award in the Island of Palmas case, 1928, p. 838; the Swiss Federal Constitution recognises state sovereignty under international law on the basis of independence, granting the state exclusive jurisdiction to make and enforce law within its territory (Art. 2 para. 1).

7 Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 292.

8 UN GGE 2013 Report, para. 20; UN GGE 2015 Report, paras. 27 and 28 b).

systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public.

Switzerland recognises that defining what constitutes a violation of the principle of sovereignty in cyberspace is particularly challenging and has yet to be clarified conclusively. It supports considering the following two criteria in such assessments: first, does the incident violate the state's territorial integrity and second, does it constitute interference with or usurpation of an inherently governmental function. A precise definition of these criteria is a question of interpretation and subject to debate. The current debate includes among other aspects i) incidents whereby the functionality of infrastructure or related equipment has been damaged or limited, ii) cases where data has been altered or deleted, interfering with the fulfilment of inherently governmental functions such as providing social services, conducting elections and referendums, or collecting taxes, and iii) situations in which a state has sought to influence, disrupt or delay democratic decision-making processes in another state through the coordinated use of legal and illegal methods in cyberspace e.g. propaganda, disinformation and covert actions by intelligence services. The assessment of an individual case depends on the nature of the cyber incident and its repercussions.

3. Prohibition of intervention

The principle of non-intervention is the corollary of the sovereign equality of all states (Art. 2 para. 1 UN Charter) and is considered customary international law.[9] In this context, intervention is understood to be the direct or indirect interference by one sovereign state in the internal or external affairs of another using coercive measures. It covers those areas where the state has exclusive jurisdiction (known as *domaine réservé*). The non-intervention principle protects a state's ability to shape its own internal affairs (political, economic, social and cultural systems) as well as its foreign policy. An infringement of sovereignty and a prohibited intervention are not the same. The latter must be coercive in nature, i.e. through its intervention a state seeks to cause another to act (or refrain from acting) in a way it would not otherwise.[10] This means that the threshold for a breach of the non-intervention principle is significantly higher than that for a violation of state sovereignty.

The prohibition of intervention is also applicable to cyberspace. This means that in cyberspace, an unlawful act of interference by one state in the political or economic affairs of another may, in addition to constituting a violation of sovereignty, also breach the non-intervention principle under international law if the respective requirements are fulfilled.[11] The distinction between exerting influence, which is permissible, and coercion, which is not, must be determined on a case-by-case basis. This is particularly true of economic coercion, which could be the case if a company that is systemically relevant was paralysed through a cyber operation. An assessment of whether the operation can be deemed coercive in nature, and thereby be in breach of the non-intervention principle, can only be made on a case-by-case basis.

---

9 Friendly Relations Declaration, A/RES/2625 (XXV), 24 October 1970; Military and Paramilitary Activities in and against Nicaragua, ICJ reports 1986, para. 202.

10 Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 202.

11 Explanatory notes to the Ordinance on Military Cyber Defence, SR 510.921.

4. Prohibition on the use of force and the right of self-defence

One of the key founding principles of the UN Charter is the prohibition on the use of force (Art. 2 para. 4). There are only two exceptions: if the use of force is authorised by the UN Security Council (Art. 42) or if the strict conditions under which the right of self-defence may be exercised are fulfilled (Art. 51).

The prohibition on the use of force and the right of self-defence are also applicable to cyberspace. The right of self-defence may only be exercised if an armed attack occurs first. In accordance with ICJ case law, not every violation of the prohibition on the use of force constitutes an armed attack, but only its gravest form. In order to qualify, the scale and effect of the attack must reach a certain threshold of gravity.[12] The ICJ has also determined that an armed attack does not necessarily have to involve kinetic military action or the use of weapons because the means by which an attack is perpetrated is not the decisive factor.[13] A state is permitted to exercise its right of self-defence in response to a cyber incident if the incident amounts in scale and effect to that of a kinetic operation in terms of inflicting death or serious injury to persons, or extensive material damage to objects. There are no binding quantitative or qualitative guidelines as to when the threshold of an armed attack in terms of scale and effect has been reached. Current discussions on how to define an armed attack in cyberspace are focusing on attacks on critical infrastructure (e.g. nuclear power plants, power grids) which reach the required threshold in terms of scale and effect i.e. serious injury to persons and/or extensive damage to objects.

The purpose of the UN Charter must guide the interpretation of the prohibition on the use of force and the right to exercise self-defence in the face of an armed attack. The Charter's objective is to maintain and, where necessary, restore international peace and security. Consequently, even if an armed attack occurs, a state is only permitted to undertake countermeasures that are necessary and proportionate in order to repel the attack. The right of self-defence only applies if the UN Security Council has not taken the necessary measures to maintain international peace and security (Art. 51 UN Charter). If the actions taken in self-defence exceed this framework, the state itself is in breach of the prohibition on the use of force. If the threshold for an armed attack has not been reached, states can have recourse to immediate and proportionate non-violent countermeasures (see section 6.2).

5. Neutrality

As a matter of principle, Switzerland considers the rights and obligations of neutral countries in international armed conflicts to be applicable to cyberspace as well.[14] If such an international armed conflict arises, a neutral country has a duty to prevent any infringements of its neutrality, such as the use of its territory by one of the conflicting parties. Parties to the conflict are obliged

---

12 Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, para. 195.

13 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 39.

14 "The Court finds that as 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 Charter), to an 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, para 89.

in turn to respect the territorial integrity of the neutral country. Therefore they may not conduct related cyber operations from installations that are either on the territory or under the exclusive control of the neutral country.[15] Parties to the conflict are also prohibited from taking control of a neutral country's computer systems in order to carry out such operations.[16]

Because of the global cross border nature of cyberspace, there are also limits to the rights and duties of a neutral country in terms of territoriality – airspace can be closed for certain flying objects, for example, but the same targeted approach cannot be used for data traffic on the internet. Another issue is that data are not only transmitted via terrestrial and cable channels but also via satellites located in outer space, which puts them outside the scope of application of the law of neutrality. Such factors must be taken into consideration when it comes to applying the rights and duties of neutral countries in cyberspace.

In principle, belligerent states are not permitted to damage the data networks of neutral countries when undertaking combat operations via their own computer networks. Neutral countries may not support conflicting parties with either troops or their own weapons. In terms of military cyber operations in connection with an international armed conflict, this means that a neutral country must prevent parties to the conflict from using its military-controlled systems or networks. In general, military networks are shielded and not publicly accessible.

6. State responsibility

The customary international rules on state responsibility are largely reflected in the draft articles issued by International Law Commission.[17] They are also applicable to cyber incidents. They provide that any state action in violation of international law shall entail the international responsibility of that state, upon which a claim for full reparation may be made. This only applies if the action can be legally attributed to the state and is deemed to constitute an internationally wrongful act, i.e. in violation of international law.

6.1. Attribution

Attribution of a cybersecurity incident refers to the identification of the perpetrator and describes a holistic, interdisciplinary process. This includes analysing the technical and legal aspects of the incident, factoring in the geopolitical context, and using the entire intelligence spectrum for the purpose of gathering information. Using this approach, a state can attribute a cyber incident to another state or a private actor, either publicly or not, and it can decide to take further political measures.

The process described above includes legal attribution, which ascertains whether a cyber incident can be legally attributed to a state and if that state can be held responsible under international law in accordance with the rules on state responsibility; it also concerns how the injured state may respond (known as countermeasures, see section 6.2). The conduct of any state organ or person exercising an inherently governmental function is always legally

---

15 Art. 2 and Art. 3 Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 18 October 1907, SR 0.515.21; Art. 2 and Art. 5 Convention Concerning the Rights and Duties of Neutral Powers in Naval War (Hague XIII), 18 October 1907, SR 0.515.22.

16 Art. 1 Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land (Hague V), 18 October 1907, SR 0.515.21.

17 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

attributable to the state concerned.[18] If a cyber incident is carried out by a non-state actor, it can only be attributed to a state under certain conditions. In such cases, state responsibility only arises if the non-state actor acts on the instructions of a state, or under the direction or control of state organs.[19] If this requirement is met, the conduct constitutes an act by the state and is attributable to that state. The injured state is also permitted to take countermeasures (see section 6.2). If the required interstate dimension is lacking however, international law does not in principle permit countermeasures against another state.

The decision to attribute conduct is at the discretion of the injured state and there is no obligation under international law to disclose the information leading to such a decision. Allegations of the organisation or implementation of an unlawful act against another state should however be substantiated.[20]

6.2. Countermeasures

A state may respond in different ways to unwelcome cyber activities carried out by another state.

Retorsion allows states to respond to such activities regardless of whether international law has been violated or not. It refers to unfriendly but lawful measures in response to unwelcome acts by another state. Typical examples of retorsion include refraining from signing a trade agreement that would benefit both parties, recalling an ambassador, or breaking off diplomatic relations as a last resort.

In cases where an act violates international law and can be legally attributed to a state, the injured state(s) may also take countermeasures in the form of reprisals, provided that the applicable rules governing state responsibility are observed.[21] Although reprisals are contrary to international law, they are justified in response to a prior breach of international law. However, such a countermeasure must not violate certain fundamental substantive obligations such as the prohibition on the use of force, fundamental human rights, most norms of international humanitarian law, peremptory norms (*jus cogens*) and the obligation to respect diplomatic and consular inviolability.[22] Military force, i.e. measures leading to loss of life and limb, are therefore prohibited.

Countermeasures must impose a (legal) disadvantage aimed at prompting the state concerned to cease its conduct that is in breach of international law and/or to make reparations. In principle, the responsible state can only impose countermeasures if it has first called for the violation(s) to cease and has announced what measures it is planning to take. Exceptions may be made for cyber operations requiring an immediate response in order for the injured state to enforce its rights and prevent further damage. Countermeasures must always be proportional, whatever the circumstances.

A countermeasure in response to a cyber incident does not necessarily have to take place in the cyber domain. In accordance with the rules governing state responsibility, other measures that aim to enforce the responsible state's compliance with its international obligations are also

---

18 Art. 4 and Art. 5 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

19 Art. 8 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

20 UN GGE 2015 Report, para. 28 f.

21 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001. Unless prohibited by international law, countermeasures are subject to strict conditions.

22 Art. 50 ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

permissible. Cyber countermeasures do not have to directly target the computer system originally used to commit the incident in question; injured states are permitted to take other measures as long as they are aimed at the responsible state ceasing its conduct that is in breach of international law. This means that depending on the specific circumstances, it may be permissible under international law to use cyber countermeasures to block the computer system abroad originally used to commit the incident. Likewise, in some cases it may be permissible to compromise computer systems abroad even if they were not the original source of the incident.

In addition to countermeasures, the rules governing state responsibility also provide for special circumstances precluding the wrongfulness of conduct that would otherwise not be in conformity with the international obligations of the state concerned. For example, a state may be exempted from complying with such an obligation if it is the only way for it to safeguard its essential interests from grave and imminent peril. Therefore the narrowly defined exceptions provided for by the rules governing state responsibility may also apply in the context of cyber operations.[23]

6.3. Due diligence

The principle of due diligence has evolved over a long period of time. Switzerland views due diligence as part of customary international law and applicable to cyberspace. The ICJ describes the concept of due diligence as a standard of conduct meaning "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[24] The doctrine of due diligence reflects fundamental principles of international law (including state sovereignty, equality, territorial integrity and non-interference).

The principle of due diligence is also applicable to cyberspace. Consequently, a state that is or should be aware of cyber incidents that violate the rights of another state is obliged to take all reasonable measures that are appropriate to stop or minimise the risks of such incidents. Due diligence is a variable standard and depends on the capacities and capabilities of a state as well as the particular circumstances of each case. Territorial states are obliged to use all reasonable means to prevent serious harm being caused to another state by activities taking place within their territory or in an area under their effective control. This makes due diligence an obligation of conduct, not of result. If the aforementioned conditions exist, the state in question is obliged under international law to close any loopholes immediately and assist in intercepting and tracing the incident.

Due diligence applies in particular to actions by private individuals that violate the rights of other states (e.g. hackers) and cannot be (clearly) attributed to the state in accordance with the rules of attribution (see section 6.1). If the aforementioned conditions exist and the state in question fails to fulfil due diligence requirements, the injured state may take countermeasures in accordance with the rules governing state responsibility in order to induce the responsible state to meet its obligations. Possible countermeasures outlined above may be taken both outside and inside the cyber domain. The responsible state may also be required to make reparations.[25]

---

[23] Chapter V, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

[24] Corfu Channel case, ICJ Reports 1949, para. 44. Due diligence is both a general principle of international law, widely recognised as part of customary international law, and a prominent legal element in various international agreements where it has been enshrined, defined and further developed (e.g. environmental law, human rights law, IHL, global health law).

[25] Art. 31, ILC Draft Articles on the Responsibility of States for Internationally Wrongful Acts, August 2001.

7. Human rights

Human rights are a cornerstone of international law. They are enshrined in a number of treaties including the UN Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). Fundamental human rights are also part of customary international law and can in part be categorised as *jus cogens*. Today, state obligations in respect of human rights have several dimensions. States must refrain from interfering with human rights (obligation to respect), protect individuals and groups against any such interference by third parties (obligation to protect) and take positive action to facilitate the enjoyment of basic human rights (obligation to fulfil).

Human rights also apply in the digital space and are a key pillar in the international regulatory framework for digitalisation. Individuals therefore have the same rights in the digital space as they do in physical space. This also applies to state security activities in cyberspace i.e. part of the digital space. Human rights obligations are equally binding upon states operating in cyberspace as in physical space. This also applies when the cyber operation in question is being carried out extraterritorially, to the extent that the States exercise their sovereign authority in doing so. If a cyber-related activity results in a violation of human rights, the victim will in principle have recourse to the enforcement mechanisms of the applicable domestic and international treaties in the same way as if the violation had been committed in physical space. Human rights monitoring bodies and tribunals can expand the scope and applicability of human rights in their practice.

A number of specific human rights may be particularly affected by cyber-related activities. An individual's right of access to information, right to privacy, or freedom of expression for example, could be restricted because of cyber operations or other cyber-related measures.

A state must be able to justify restricting these or other human rights in cyberspace based on the same rules that apply in physical space. In principle, any act of state interference requires an adequate legal basis. The state must also be able to demonstrate that in the balance of interests its actions are appropriate, necessary and reasonable in order to meet a legitimate objective.

Switzerland considers the applicability of human rights to cyberspace to be an unequivocal principle. However, new questions may arise when considering how this applies in individual cases. For example, if cyber-related activities are used to block access to social media, the question of freedom of expression may need to be clarified – at what point can this legally protected right be interfered with? Can the individual continue to exercise this right through alternative communication channels? To what extent are private actors also bound by human rights obligations? Human rights bodies need to develop their work in this field in order to ensure the application of human rights in cyberspace.

II. International humanitarian law

Switzerland considers international law to be applicable to cyberspace, which includes the application of IHL in the context of armed conflicts. Switzerland's foreign policy priorities include ensuring respect as well as strengthening and promoting IHL. Switzerland is well known for its neutrality, humanitarian tradition and role as depositary of the Geneva Convention. This position paper therefore addresses IHL issues in greater depth.

1. Applicability of IHL

IHL is applicable once an international or non-international armed conflict de facto exists. It is applicable in any armed conflict and to all parties to a conflict. IHL addresses the realities of war without considering the reasons for or the legality of the use of force. It does not deal with the legality of war, nor does it legitimise the use of force between states. [26] The purpose of IHL is to regulate the conduct of hostilities and to protect victims of armed conflict, in particular by restricting the use of certain means and methods of warfare. The ICJ clearly stated that the established principles and rules of IHL apply to "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future". [27]

This is applicable to cyberspace in the same way as for traditional and new operational spaces (outer space, airspace, land, maritime space, electromagnetic space, information space). IHL is therefore the main body of international law governing cyber operations that have a connection with an armed conflict. Implementing IHL effectively contributes to ensuring international security. Existing IHL, particularly its fundamental principles, places important limits on the execution of cyber operations in armed conflicts.

2. Fundamental IHL provisions regulating the conduct of hostilities

2.1. Principle concerning the means and methods of warfare

IHL prohibits or restricts means (weapons) and methods of warfare through general principles – regulating conduct or prohibiting certain effects – and specific rules addressing particular means and methods of warfare. As regards weapons, IHL distinguishes between the legality of a particular type of weapon (weapons law) and the legality of how it is used (law of targeting). The inherent characteristics of certain weapon categories entail that their use – in some or all circumstances – is unlawful *per se*. The admissibility of all other weapons depends on whether their use is in conformity with IHL.

This is also applicable to cyberspace. In fact, developing or using new means and methods of warfare must be in compliance with existing international law, particularly IHL. This is true even if a weapon is not covered by a specific norm and the treaty provisions governing the conduct of hostilities do not explicitly refer to new technologies. The customary rules of IHL apply equally to all means and methods of warfare, including in cyberspace. Indeed, it is a long standing principle that the right of parties to an armed conflict to choose methods or means of warfare is not unlimited.

2.2. Legality of a particular type of weapon

IHL stipulates that any means or method of warfare possessing one or more of the following characteristics is inherently unlawful if:

(1) it is of a nature to cause superfluous injury or unnecessary suffering;

---

[26] Any use of force between states is governed by the UN Charter and relevant customary international law (see above, section 1.4).

[27] Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, para. 86; "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."

(2) it is indiscriminate by nature, because it cannot be directed against a specific military objective or its effects cannot be limited as required by IHL;
(3) it is intended, or may be expected, to cause widespread, long-term or severe damage to the natural environment; or
(4) it is specifically prohibited by treaty or customary international law.

This is applicable to cyberspace and, therefore, to cyber means and methods of warfare.

2.3. Legality of the manner in which the weapon is employed

With regard to the lawful use of cyber means and methods of warfare, the rules and principles governing the conduct of hostilities must be respected. Belligerents must in particular comply with the principles of distinction, proportionality and precaution by:

(1) distinguishing between military objectives on the one hand, and civilians or civilian objects on the other hand and, in case of doubt, presume civilian status;
(2) evaluating whether the incidental harm expected to be inflicted on the civilian population or civilian objects would be excessive in relation to the concrete and direct military advantage anticipated from that particular attack;;
(3) taking all feasible precautions to spare civilians and civilian objects.

This is also applicable in cyberspace, when using cyber means and methods of warfare. The aforementioned principles are applicable in particular to cyber operations that amount to an attack within the meaning of IHL i.e. acts of violence against the adversary, whether in offence or defence. What exactly constitutes a 'cyber attack' in an armed conflict has yet to be clarified. It encompasses at the very least cyber operations that are reasonably expected to cause, directly or indirectly, injury or death to persons, or physical damage or destruction to objects. The question, how exactly data is protected in the absence of such physical damage, remains a challenge. In practice, a responsible actor should generally be able to assess the potential impact of their actions and any resulting damage. As this estimation depends, amongst other things, largely on the information available at the time when decisions about an operation are taken, the obligation to take all precautionary measures practically possible to spare civilians and civilian objects plays a particularly important role in the use of cyber means and methods of warfare.

3. Other IHL provisions

Full compliance with IHL is not limited to the rules and principles governing the conduct of hostilities. There are other specific rules of IHL that must be respected, including when conducting military operations that do not qualify as an 'attack'. For example, certain categories of persons and objects are subject to special protection, such as medical, religious or humanitarian personnel and objects, which must be respected and protected in all circumstances.

This is also applicable to cyberspace. For cyber operations that are linked to any of these specially protected persons or objects, or to other activities governed by IHL, all of the relevant, specific rules must be observed.

4. Ensuring respect for IHL

States and parties to a conflict have an overarching obligation to “respect and ensure respect” for IHL “in all circumstances”. It is uncontested that preparatory measures must be taken to

implement IHL and that its implementation needs to be supervised. This requires states and parties to a conflict, inter alia, to take measures to ensure that the development and use of means and methods of warfare fully comply with IHL, and to prevent outcomes that would be unlawful.

This is also applicable to cyberspace and the cyber means and methods of warfare. As with any other weapon, means or method of warfare, States have the positive obligation to determine, in their study, development, acquisition or adoption, whether their employment would, in some or all circumstances, violate existing international law.. In this regard, the obligation to assess the legality of a new weapon as set out in Art. 36 of Additional Protocol I to the Geneva Conventions[28] is an important element to prevent or restrict the development and employment of new cyber weapons that would fail to meet in particular the obligations set out above.

[28] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1), SR 0.518.521.