Position Paper of the Republic of Austria:
Cyber Activities and International Law

April 2024

Table of Contents
1. General Remarks .................................................................................................................. 3
2. Introduction .......................................................................................................................... 3
3. State Sovereignty .................................................................................................................. 4
4. Prohibition of Intervention ............................................................................................... 5
5. Prohibition of the Threat or Use of Force ........................................................................ 6
6. The Right of Self-Defence .................................................................................................. 7
7. State Responsibility ............................................................................................................. 8
8. Due Diligence ..................................................................................................................... 10
9. Peaceful Settlement of Disputes ....................................................................................... 11
10. Human Rights ................................................................................................................... 12
11. Diplomatic and Consular Missions, International Organisations and Data Embassies .. 14
12. International Humanitarian Law (IHL) ........................................................................... 16
13. International Criminal Law ............................................................................................... 20
14. Neutrality .......................................................................................................................... 21
**List of Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARSIWA</td>
<td>Articles on Responsibility of States for Internationally Wrongful Acts</td>
</tr>
<tr>
<td>Art.</td>
<td>Article</td>
</tr>
<tr>
<td>BGBl.</td>
<td>Austrian Federal Law Gazette (<em>Bundesgesetzblatt</em>)</td>
</tr>
<tr>
<td>cf.</td>
<td>confer</td>
</tr>
<tr>
<td>CFSP</td>
<td>Common Foreign and Security Policy</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention on Human Rights</td>
</tr>
<tr>
<td>ECSCCR</td>
<td>International Covenant on Economic Social and Cultural Rights</td>
</tr>
<tr>
<td>e.g.</td>
<td>for example (<em>exempli gratia</em>)</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GC</td>
<td>Geneva Convention</td>
</tr>
<tr>
<td>GGE</td>
<td>Group of Governmental Experts</td>
</tr>
<tr>
<td>IAC</td>
<td>international armed conflict</td>
</tr>
<tr>
<td>ICC</td>
<td>International Criminal Court</td>
</tr>
<tr>
<td>ICCPR</td>
<td>International Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ICJ</td>
<td>International Court of Justice</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and communications technology</td>
</tr>
<tr>
<td>ICTY</td>
<td>International Criminal Tribunal for the former Yugoslavia</td>
</tr>
<tr>
<td>Ibid.</td>
<td>as above (<em>ibidem</em>)</td>
</tr>
<tr>
<td>i.e.</td>
<td>that is (<em>id est</em>)</td>
</tr>
<tr>
<td>IHL</td>
<td>International Humanitarian Law</td>
</tr>
<tr>
<td>IO</td>
<td>International Organisation</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NIAC</td>
<td>non-international armed conflict</td>
</tr>
<tr>
<td>Nr.</td>
<td>number</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>p.</td>
<td>page</td>
</tr>
<tr>
<td>para.</td>
<td>paragraph</td>
</tr>
<tr>
<td>Rep</td>
<td>Report</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNGA</td>
<td>United Nations General Assembly</td>
</tr>
<tr>
<td>UNGP</td>
<td>United Nations Guiding Principles on Business and Human Rights</td>
</tr>
<tr>
<td>VCCR</td>
<td>Vienna Convention on Consular Relations</td>
</tr>
<tr>
<td>VCDR</td>
<td>Vienna Convention on Diplomatic Relations</td>
</tr>
</tbody>
</table>
1. General Remarks

This position paper provides a non-exhaustive overview of Austria’s position on the application of international law to cyber activities. It is the product of years of Austrian practice and statements at various international fora, dedicated to clarifying the application of international law to cyber activities. For the preparation of this paper, the position papers and views of States, academics and other stakeholders were also analysed.¹ In the light of future developments and discussions, this paper may be subject to further revisions. In this paper, all references to “cyberspace” have been deliberately omitted in view of the fact that all cyber activities do not take place in a separate “virtual space”, but in the real world.

2. Introduction

<table>
<thead>
<tr>
<th>Key Positions:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>International law</strong> applies in its entirety to cyber activities.</td>
</tr>
<tr>
<td><em>Austria sees no need</em> for the development of a <strong>new legally binding instrument</strong> relating to international cyber activities.</td>
</tr>
<tr>
<td><em>Any legal assessment</em> of a cyber-related event or incident depends on the examination of the relevant circumstances in each <strong>individual situation</strong>, especially given the complexity that the cyber context often entails.</td>
</tr>
</tbody>
</table>

Austria is committed to international law and the rule of law in and outside the cyber context. Therefore, Austria is of the opinion that international law applies in its entirety to cyber activities. Indeed, all UN Member States agreed by consensus that international law, and in particular the Charter of the United Nations, applies to cyber activities.² It is for this reason that Austria, for the time being, does not see a need for the development of a new legally binding instrument relating to international cyber activities. However, future technological developments may require further clarification on the application of international law to cyber activities.

In this context, it is important to emphasize that the voluntary non-binding norms, rules and principles recommended by the GGE³, endorsed by the UN General Assembly (UNGA) in 2015,⁴ and reaffirmed several times thereafter, are an important set of commitments dedicated to responsible state behaviour in the cyber context. In Austria’s view, these non-binding norms,

---


rules and principles do not undermine, change or replace the legally binding rules of international law, but confirm and complement them.

For the purpose of this position paper, the term “cyber activities” is understood to refer to the activities carried out by or attributable to states, using information and communications technology (ICT) and infrastructure.

3. State Sovereignty

Key Positions:
Respect for the sovereignty of other states is a binding rule of customary international law that also applies to cyber activities. States exercise sovereignty over ICT infrastructure on, and persons engaged in cyber activities in, their territory. Sovereignty also entails obligations for states concerning cyber activities, in particular with regard to the observance of human rights and fundamental freedoms.

Austria takes the position that respect for state sovereignty is a binding rule of customary international law that also applies to cyber activities. This means that a cyber activity may violate a state’s sovereignty, even if it does not reach the threshold of, inter alia, an unlawful intervention or threat or use of force. The violation of state sovereignty, through cyber activities of a state or attributable to it, entails the international responsibility of the acting state.

State sovereignty entails specific rights – such as a state’s right to exercise exclusive jurisdiction over ICT infrastructure on, and persons engaged in cyber activities in, their territory – and obligations – such as the obligation to respect the sovereignty of other states, also with regard to lawful cyber activities. A state’s sovereignty must not be used as a pretext for a state to infringe its human rights obligations, including on data protection and privacy, freedom of expression, and freedom of information.

A cyber activity violates the sovereignty of another state when it violates a state’s territorial integrity, as well as when it constitutes an interference with or usurpation of an inherently governmental function of a state. Cyber activities that result in physical damage or injury certainly constitute a violation of state sovereignty. Other – only limited – intrusions leading to, e.g. the temporary loss of functionality of critical infrastructure within a state or a cyber activity that temporarily prevents access to essential governmental services, may also constitute a violation of sovereignty. Similarly, cyber espionage activities, including industrial cyber espionage against corporations, within a state’s territory may also violate the state’s sovereignty.5

5 On surveillance or espionage activities, see also Chapter 11.
The mere traversing of data packages – conducted by a state or otherwise attributable to it - through the ICT infrastructure of another state, without negatively affecting the functioning of such infrastructure, does not in itself violate the principle of sovereignty.

Example: State A initiates a cyber espionage activity against the Foreign Ministry of state B for the purpose of obtaining illegal access to the internal communication and information system. When state B discovers that its system is compromised, it is required to conduct a total shutdown of the system and temporarily establish an alternative while the IT system is cleaned and restored. Such a cyber activity would constitute a violation of state B’s sovereignty.

4. Prohibition of Intervention

Key Position:
The customary international law rule prohibiting intervention, i.e. coercive interference, by one state in the internal or external affairs of another state also applies to cyber activities.

The customary international law rule of non-intervention prohibits the coercive interference in the internal or external affairs (“domaine réservé”) of another state. It was affirmed in various declarations of the UNGA, including the Friendly Relations Declaration.6

As was held by the International Court of Justice (ICJ) in the Nicaragua case, the internal or external affairs of a state include matters in which each state is to decide freely, such as its “choice of a political, economic, social and cultural system, and the formulation of foreign policy”.7

Coercion occurs when a state seeks to compel another state to change its behaviour with respect to its internal or external affairs, i.e. to force that state to act in an involuntary manner or involuntarily refrain from acting in a particular way. Coercion is most evident in an intervention using force.8 However, also non-forcible forms of interference can be coercive. The assessment of whether a cyber activity constitutes a coercive interference requires a case-by-case analysis. For instance, a cyber activity that interferes with a state’s ability to hold elections or which manipulates election results could, if undertaken to compel a state to involuntarily change a government policy, constitute a violation of the prohibition of intervention. Large-scale cyber activities, including disinformation campaigns, conducted by or attributable to a state may also constitute, if undertaken to compel another state to involuntarily change its behaviour, a violation of the prohibition of intervention.

7 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States) (Merits) [1986] ICJ Rep 14, para. 205.
8 Ibid.
It is important to distinguish such disinformation campaigns from lawful public relations activities of state representatives, including e.g. by openly criticising the human rights situation in another state on social media accounts or websites.

A cyber activity that does not reach the threshold of a prohibited intervention may still constitute a violation of state sovereignty (see Chapter 3).

Example: State A launches a large-scale campaign against the government of state B that spreads disinformation about the alleged corrupt business practices of state B’s government, intended to sow distrust within the population of state B. The campaign eventually causes the government of state B to resign, resulting in a governmental crisis. Such a cyber activity would violate the prohibition of intervention.

5. Prohibition of the Threat or Use of Force

Key Positions:
The prohibition of the threat or use of force, as enshrined in Art. 2 para. 4 UN Charter, which is a *ius cusancis norm* of customary international law, applies to cyber activities.
A cyber activity may constitute a threat or use of force, and hence a violation of the UN Charter, if the scale and effects of the actual or threatened cyber activity are or would be comparable to those of a conduct using kinetic means.

Art. 2. para. 4 UN Charter, which is a peremptory norm (*ius cogens*) and a rule of customary international law, stipulates that states “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”. A threat or use of force is only permitted in the exercise of a state’s right to self-defence (Art. 51 UN Charter), in the event of a Security Council authorization, or with the consent of the affected state.

According to its advisory opinion on nuclear weapons, the ICJ confirmed that Art. 2 para. 4 UN Charter applies “to any use of force, regardless of the weapons employed.”

A cyber activity constitutes a threat or use of force if its scale and effects are or would be comparable to those of a kinetic threat or use of force. For instance, a cyber activity that leads to injury, death or significant physical damage constitutes an unlawful use of force. Cyber activities causing non-physical damage may also constitute an unlawful use of force. Moreover, a cyber activity could either be part of a wider operation using force with kinetic means, an independent use of force with physical effects, or an independent use of force without physical effects.

---

When a cyber activity does not reach the threshold of a threat or use of force, it may nevertheless constitute a prohibited intervention or violation of state sovereignty.

Example: State B conducts a cyber activity against an electric power station situated in state A, on which a large part of state A’s population and governmental infrastructure relies. As a result, the power station is severely damaged, causing a blackout for several hours until power supply can be restored. Such a cyber activity would constitute an unlawful use of force.

6. The Right of Self-Defence

Key Positions:
A cyber activity may constitute an **armed attack** within the meaning of **Art. 51 UN Charter** whenever the scale and effects of the activity are comparable to those of an armed attack using kinetic means.

In response to a cyber activity constituting an armed attack a state may exercise its inherent right of self-defence.

The **response** to such a cyber activity is **not limited to cyber means**. Similarly, the response to an armed attack using kinetic means may include cyber means.

The response must be **necessary and proportionate in order to end the attack**.

The inherent right of individual or collective self-defence against an imminent or ongoing armed attack is a rule of customary international law, codified in **Art. 51 UN Charter**, and enables a state to respond in a necessary and proportionate manner. Any measure – also through cyber means – taken by the responding state must be immediately reported to the UN Security Council.

Not every use of force constitutes an armed attack in the sense of **Art. 51 UN Charter**10, both in the kinetic and the cyber context. An armed attack exists when force is used on a relatively large scale, is of sufficient gravity and has a substantial effect. A cyber operation constitutes an armed attack if, as in the kinetic context, it causes significant death or injury to persons, or substantial material damage or destruction. This is, however, also context-dependent and subject to a case-by-case analysis. An armed attack can also consist of a series of attacks.11 Likewise, while one cyber activity in isolation may not constitute an armed attack, several cyber activities may still constitute such an attack if, taken together, they are sufficiently grave to reach the threshold of an armed attack.

Armed attacks can be committed both by state and non-state actors. Given the fact that most cyber activities are not carried out by state authorities, it is important to note that acts of non-

---


11 *Cf. Oil Platforms (Iran v. United States) (Merits)* [2003] ICJ Rep 4, para. 64 ; *Nicaragua (Merits)* para. 231.
state actors can amount to an armed attack in the sense of Art. 51 UN Charter, provided that the following two conditions are fulfilled: 1) there is a “transboundary element”, e.g. the non-state actor operates from the jurisdiction of another state; and 2) the other state is harbouring or otherwise substantially supporting the operations of the non-state actor under its jurisdiction, or is unable, as a consequence of the complete absence of state authority and effective control over the respective territory, to prevent or suppress the non-state actor’s operations.

7. State Responsibility

**Key Positions:**
The customary international law rules on state responsibility also apply to cyber activities by states.

A state incurs international responsibility for acts or omissions related to a cyber activity that are attributable to that state and that constitute a breach of an international legal obligation of that state.

The attribution of cyber activities to a state must be made in accordance with the customary international law rules on state responsibility.

Internationally wrongful acts attributable to a state, including acts in the cyber context, may be answered by countermeasures, including through cyber means. The same limitations to countermeasures apply as in non-cyber-related contexts.

The customary international law rules of state responsibility, largely codified in the International Law Commission’s Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), apply to cyber activities that are attributable to states. According to the law of state responsibility, every internationally wrongful act – i.e. an act or omission that is attributable to a state under international law and constitutes a breach of an international obligation of the state – entails the international responsibility of that state (cf. Art. 1 and 2 ARSIWA).

A cyber activity is attributable to a state if it is conducted by a de jure or de facto state organ, a person or entity exercising elements of governmental authority, an organ placed at the disposal of a state by another state, or by a non-state actor acting on the instructions of, or under the direction or effective control \(^{12}\) of a state (Art. 4, 5, 6 and 8 ARSIWA). Ultra vires acts by state organs are generally also attributable to the state, as well as conduct which was acknowledged and adopted by a state as its own (Art. 7 and 11 ARSIWA).

The responsible state must cease a continuing act or offer assurances and guarantees of non-repetition under certain circumstances, as well as make full reparation for the injury caused by the wrongful act (Art. 30 and 31 ARSIWA).

The wrongfulness of a cyber activity may, under some circumstances, be precluded if it was taken in self-defence, or by way of a non-forcible countermeasure, or in situations of force majeure, distress or necessity (Art. 21 to 25 ARSIWA). A state may also respond with lawful retributions, which themselves are unfriendly, but lawful acts.

**Countermeasures**

An injured state may resort to countermeasures in order to compel the responsible state to cease its internationally wrongful conduct and to make full reparation. In particular, cyber countermeasures or countermeasures in response to a cyber activity must not affect the prohibition of the threat or use of force and other peremptory norms (Art. 50 ARSIWA), and must be proportionate (Art. 51 ARSIWA). In addition, a state must call on the responsible state to cease the wrongful conduct and provide reparation, as well as notify the responsible state of its decision to take a countermeasure if the responsible state does not comply with its obligations. However, in case of urgent countermeasures, which may be particularly necessary in the context of a cyber countermeasure, the notification requirement may not apply (Art. 52 ARSIWA).

In addition, Austria holds the view that states may also take collective countermeasures against a state that breaches an obligation erga omnes, i.e. an obligation owed to the international community as a whole (cf. Art. 48 para. 1(a) and Art. 54 ARSIWA), e.g. against a state that commits acts of aggression or genocide, especially if the directly injured state has requested the assistance of other states. Cyber activities would rarely breach such an obligation. However, a public cyber campaign attributable to a state that calls for acts of violence against a national, ethnical, racial or religious group with the intention to destroy this group, could amount to public incitement to commit genocide in violation of Art. III (c) of the Genocide Convention. However, in such cases, the principle of proportionality (Art. 51 ARSIWA) poses significant limitations to the exercise of collective countermeasures and must at all times be taken into account.

Preventive cyber measures, prior to the commission of an internationally wrongful act conducted by or attributable to a state, such as exploiting vulnerabilities in other states’ ICT networks and placing “logic bombs” therein, cannot be justified under the law of state responsibility.

---

13 See supra, Chapter 6.
14 Institut de Droit International, Resolution ‘Obligations erga omnes in international law’ (August 2005).
8. Due Diligence

Key Positions:
States are under an obligation to ensure that their territory is not knowingly used for cyber activities contrary to the rights of other states.

A state that is or should be aware of such a cyber activity emanating from its territory has a due diligence obligation to take all reasonable measures that are appropriate to prevent the violation and end the activity.

According to the ICJ in the Corfu Channel Case, each state is obligated “not to allow knowingly its territory to be used for acts contrary to the rights of other States.” This general due diligence obligation of a state concerning its territory is an obligation of conduct, not of result, and is also applicable to cyber activities.

If a state has or should have knowledge of a cyber activity contrary to the rights of other states emanating from ICT infrastructure on its territory, it has to take all reasonable measures that are appropriate to prevent the violation and end the activity.

While – in addition to actual knowledge – the obligation comprises also situations in which a state should have known about the activities in question, it cannot be concluded from the mere fact of the control exercised over its territory that a state necessarily knew, or ought to have known, of any unlawful act perpetrated therein.

The required “reasonable measures” are to be assessed in accordance with the due diligence obligation of the territorial state: Due diligence constitutes an “objective” international standard of vigilance and care which is reasonably expected from an average “good government” that is mindful of its international obligations and acting in good faith, in the light of the potential risks in a given situation. Due diligence is a variable standard that may change as a result of new technological developments or changes in risk assessment.

In the cyber context, it first includes the obligation of a state to put in place a minimum governmental ICT infrastructure and capacity, enabling it to exercise the necessary degree of diligence with regard to cyber activities on its territory. Second, when a state becomes aware or should be aware of a cyber activity emanating from its territory that violates the rights of another state, it is under an obligation, in light of its capacity, to take all measures that can be reasonably expected from an average state in the given situation and are appropriate to

---

16 The Corfu Channel Case (United Kingdom v. Albania) (Merits) [1949] ICJ Rep 4, p. 22.
17 Ibid., p.18.
18 See generally International Law Association, Second Report on Due Diligence in International Law (July 2016); Oxford Institute for Ethics, Law and Armed Conflict, Research Project on Cyber Due Diligence by Dapo Akande, Talita Dias and Antonio Coco, Project Report , Cyber due diligence in international law (March 2021).
prevent the violation and end the activity. At a minimum, it entails the obligation to inform the injured state of the cyber activity.

The *due diligence* obligation does not entail that a state has to monitor ICT infrastructure located on its territory at all times. Nor may this obligation be used in any way as an excuse to infringe on human rights.

Example: State A is aware of a criminal hacker group operating on its territory and targeting other states. The group is conducting a cyber attack against state B, encrypting all the files of state B’s Ministry of Foreign Affairs and requesting a ransom payment. State B is able to trace the activity to state A, but is unable to clearly attribute the attack to state A. It notifies state A of the cyber activity by the group emanating from state A’s territory. State A rejects the allegation and refuses to investigate the conduct on its territory. Thereby, state A violates its *due diligence* obligation.

9. Peaceful Settlement of Disputes

**Key Position:**
The obligation of states to settle their international disputes by peaceful means extends to disputes involving cyber activities by states that might endanger international peace and security.

A key principle stipulated in Art. 2 para. 3 and 33 UN Charter is the obligation of states to settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered. This obligation is equally applicable in the cyber context. Settling disputes by peaceful means entails that states do not prematurely reach to measures which may have the potential to escalate a given situation.

It is also important to highlight the role of the Security Council and the General Assembly in the pacific settlement of disputes, as further laid out in Chapter VI of the UN Charter.

Art. 33 para. 1 UN Charter provides examples of peaceful settlement methods, such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, or resort to regional agencies or arrangements. In this context, the ICJ plays an important role in settling disputes peacefully through judicial means. All states should therefore recognize the ICJ’s compulsory jurisdiction in accordance with Art. 36 of the ICJ Statute. Art. 33 is non-exhaustive, meaning that states can also resort to other peaceful means, if they are more suitable for the dispute at hand.
10. Human Rights

Key Positions:

International human rights law is applicable to cyber activities; human rights obligations are equally binding upon states’ cyber activities, and individuals have the same rights as they do outside of the cyber context.

The same rights that people have offline must also be protected online.¹⁹ States are also obligated to ensure respect for human rights with regard to cyber activities by third parties, including business enterprises.

States are bound by international human rights law also in respect of cyber activities. The same rights that individuals enjoy “offline” must be protected “online”. Also in this regard, states are bound by their human rights obligations as laid down in international instruments, in particular UN treaties such as the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic Social and Cultural Rights (ECSCR), relevant regional instruments, in the case of Austria the European Convention on Human Rights (ECHR) and its protocols, the European Social Charter and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as customary international law. The concept of jurisdiction under human rights law is not altered with respect to cyber activities.

States must not restrict the right to privacy (Art. 17 ICCPR and Art. 8 ECHR), freedom of expression, including the freedom to seek, receive and impart information (Art. 19 ICCPR and Art. 10 ECHR – which include a right to internet access), as well as the right to freedom of association (Art. 22 ICCPR and Art. 11 ECHR) as a result of cyber activities or other cyber-related measures. Those rights may be particularly affected through disinformation campaigns as well as unlawful surveillance activities.

In the light of their human rights obligations, states should support the promotion of a secure, open and free internet.

Restrictions of Human Rights in the Cyber Context

States must justify restrictions on human rights with respect to cyber activities on the basis of the same rules relevant for restrictions in other contexts. Any interference with human rights requires a legal basis, must pursue a legitimate aim, and must be necessary and proportionate to the aim pursued. The temporary suspension of a limited number of human rights may be permissible in an emergency situation.

However, certain cyber activities are particularly problematic in view of human rights obligations of states, due to their indiscriminate and particularly invasive nature. This includes

mass surveillance, in particular biometric mass surveillance, internet shutdowns, domain blocking, and the use of spyware against journalists, activists, and human rights defenders.

In addition, other applications of emerging technologies – such as remote biometric identification systems including facial recognition technologies, emotion recognition technologies and social scoring systems – raise serious concerns as to their compatibility with international human rights law and may be deployed only under very restricted conditions with sufficient safeguards to avoid abuse.

Lastly, the principle of sovereignty must not be used as a pretext to infringe on individuals’ human rights.

**Business and Human Rights**

As a positive obligation, states must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. While states are the primary obligated parties, business enterprises, regardless of their size, industry, operational context and structure, are also required to respect human rights.

The United Nations Guiding Principles on Business and Human Rights (UNGP)\(^{20}\) and the OECD Guidelines\(^{21}\), while not legally binding, provide guidance to companies on how to comply with their due diligence obligations and how to avoid potential negative impacts of their business activities on human rights.

According to the UNGP, business enterprises have a responsibility to respect human rights. This requires them to avoid causing or contributing to adverse human rights impacts through their own activities. Important steps in this context include implementing human rights due diligence policies, as well as seeking to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they themselves have not contributed to those impacts.

Within their jurisdiction, states must hold third parties, including business enterprises such as technology companies, accountable if their operations, products or services lead to human rights abuse through harmful cyber activities.

---


11. Diplomatic and Consular Missions, International Organisations and Data Embassies

**Key Positions:**
ICT infrastructure on the premises of a diplomatic or consular mission, a “data embassy”, or the seat of an international organisation (IO), enjoys inviolability. Archives, documents and official correspondence of a diplomatic or consular mission, or an IO, that are in electronic form are inviolable. Diplomatic and consular missions, as well as IOs (subject to the provisions of their headquarters agreements) must not engage in cyber activities contrary to the laws and regulations of the receiving state, including espionage activities, and must not interfere in the internal affairs of that state. In addition, their premises must not be used to engage in cyber activities that are incompatible with their functions.

**Diplomatic and Consular Missions**

Diplomatic and consular missions enjoy inviolability of their premises under customary international law, as codified in the Vienna Convention on Diplomatic Relations (VCDR), and the Vienna Convention on Consular Relations (VCCR), respectively. The premises of a mission are inviolable and must not be entered by agents of the host state except with consent by the head of mission. In addition, any property located within the mission – including ICT infrastructure – is immune from search, requisition, attachment or execution. This means that also remote access to the ICT infrastructure located within the mission without express consent is prohibited.

Moreover, archives and documents, as well as official correspondence of the mission, also in electronic form, are inviolable wherever they are located. Furthermore, the receiving state has a duty to permit free communication on the part of the mission for all purposes.

It is the duty of all persons enjoying privileges and immunities to respect the laws and regulations of the receiving State and not to interfere in the internal affairs of that State. In addition, the premises of the mission must not be used in a manner incompatible with the functions of the mission, or with other rules of general international law or any special agreements in force between the sending and the receiving State. In the cyber context, this also means that persons enjoying privileges and immunities must not engage in unlawful surveillance or espionage activities in the receiving state, and the premises of the mission must also not be used for such purposes.

---

22 Art. 22(1) VCDR, Art. 31(2) VCCR.
23 Art. 22(3) VCDR.
24 Art. 24 and Art. 27(2) VCDR.
25 Art. 27(1) VCDR and Art. 35(1) VCCR, respectively.
26 Art. 41(1) VCDR, Art. 55(1) VCCR.
27 Art. 41(3) and Art. 3 VCDR, Art. 55(2) and Art. 5 VCCR.
The receiving state has the duty to take all appropriate steps to protect the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.\(^{28}\) Thus, a state that becomes aware of a malicious cyber activity against a diplomatic or consular mission in its territory, has to take all appropriate steps to protect the mission from such an activity.

**International Organisations**

Similar rights and obligations apply in the context of IOs, to the extent they are specified in the headquarters agreements between the host state and the IO. The premises of the IO are inviolable and shall not be entered by agents of the host state, except with the consent of the head of the IO.\(^{29}\) This also entails that remote access to the ICT infrastructure within the premises of the IO is prohibited.

All officials of IOs and state representatives have a duty to respect the laws and regulations of the host state and not to interfere in the internal affairs of that state. This means that these persons must not engage in unlawful surveillance or espionage activities in the host state, and the premises of the IO must not be used for such purposes.

Host states also have a duty to protect the premises of the IO from outside disturbances or unauthorized entry.\(^{30}\) Thus, if a state becomes aware of a malicious cyber activity against an IO situated on its territory, it has to take all appropriate steps to protect the IO from such an activity. In this regard, Austria is working closely with IOs situated on its territory.

**“Data Embassies”**

In some cases, ICT infrastructure may enjoy inviolability under treaty or customary international law as applicable. Recently, some states and IOs have concluded agreements with other states which enable a state (i.e. the sending state) or an IO to store or process data in the territory of another state (i.e. the receiving state).\(^{31}\) It is important to note that such bilateral agreements are only binding upon the parties involved, and not on third parties.

---

\(^{28}\) Art. 22(2) VCDR, Art. 31(3) VCCR.

\(^{29}\) Cf. Agreement between the Republic of Austria and United Nations Regarding the Seat of the United Nations in Vienna, available at: [https://www.un-ilibrary.org/content/books/9789210457385s002-c052/read](https://www.un-ilibrary.org/content/books/9789210457385s002-c052/read), Section 17.

\(^{30}\) Ibid., Section 18.

However, a cyber activity that causes the destruction of governmental data in the data embassy of state A in the territory of state B, may be considered a violation of sovereignty of both state A and state B.\textsuperscript{32}

12. International Humanitarian Law (IHL)

a. Applicability of IHL to Cyber Activities

| Key Position: |
| IHL applies to all cyber activities carried out in connection with an armed conflict. IHL seeks to limit the effects of armed conflicts and to protect those who do not, or no longer, participate in hostilities, in particular civilians. |
| IHL applies to a particular cyber activity if there is a sufficient nexus between the armed conflict and the cyber activity. |

The obligation to respect and to ensure respect for IHL in all circumstances (cf. Common Art. 1 of the Geneva Conventions of 1949 (GCs)) applies in the context of cyber activities carried out in connection with an armed conflict.

IHL applies to a particular cyber activity if there is a sufficient nexus between the armed conflict and the cyber activity, i.e. the cyber activity must be undertaken by one party to the conflict against the other party and must contribute to the former party’s military effort.

Affirming the applicability of IHL to cyber activities in connection with an armed conflict does not encourage or legitimize cyber warfare. IHL intends to protect civilians and civilian objects from the effects of hostilities.

Cyber activities in connection with an armed conflict are subject to the same geographical limitations as in the kinetic context, despite particular challenges due to the general cross-border nature of cyber activities.

b. Existence of an Armed Conflict

| Key Positions: |
| International armed conflicts (IAC) and non-international armed conflicts (NIAC) may be partially or entirely conducted through cyber activities. |

An international armed conflict (IAC) is characterized by armed hostilities between two or more states. A non-international armed conflict (NIAC) is characterized by protracted armed hostilities between the armed forces of a state and organized non-state armed groups or

\textsuperscript{32} See supra, Chapter 3.
among such groups. Armed hostilities in the context of an IAC exist whenever there is “resort to armed force between States”. As such, an IAC is, in any case, triggered where cyber activities between states cause physical effects similar to those of kinetic means such as destruction, death or injury.

**Example 1:** State A launches a cyber activity against the power grid of state B, which causes the power grid to collapse. The collapse entails foreseeable complications in medical and humanitarian facilities, leading to the death of a significant amount of persons.

**Example 2:** State B conducts a cyber activity against state A to open the floodgates of a water reservoir in state A, and which results in a foreseeable flood causing significant damage to property and civilian casualties in state A.

Both above-mentioned examples trigger an IAC.

A NIAC exists when there are protracted armed hostilities between government authorities and organized armed groups, or between such armed groups, within a state. Thus, to qualify as a NIAC, the violence must reach a level of intensity, and the armed groups must have a minimum degree of organization. Provided these requirements are fulfilled, cyber activities by themselves are sufficient to trigger a NIAC.

c. **The Meaning of “Attack” under IHL**

**Key Position:** Cyber activities may amount to attacks within the meaning of IHL, i.e. acts of violence against the adversary, whether in offense or defense (Art. 49 Additional Protocol I).

The term “attack” within the meaning of IHL should be interpreted broadly, pursuant to an effects-based approach. Accordingly, a cyber activity that is reasonably expected to cause injury or death to persons or damage or destruction to objects constitutes an attack within the meaning of IHL. However, also a cyber activity that is designed to disable, either in a kinetic or non-kinetic context, an ICT network of the adversary during an armed conflict, may constitute an attack as defined in IHL. Such a disablement may have grave indirect/reverberating effects that, for instance, undermine the state’s functioning as a whole or critical national interests.

Cyber activities carried out in connection with an armed conflict that do not amount to attacks may nevertheless qualify as other military operations, which are also subject to limitations under IHL.

---

33 Prosecutor v Duško Tadić a/k/a “Dule” (Decision on the defence motion for interlocutory appeal on jurisdiction) ICTY-94-1 (2 October 1995) [70].

34 Protocol I Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts.
d. Core Principles of IHL

**Key Position:**
The core principles of IHL, such as the *principles of humanity, distinction, military necessity, proportionality and precautions in attack*, apply to attacks through cyber activities in IACs as well as NIACs.

Among the core principles of IHL, the principles of distinction and proportionality are particularly important in the cyber context.

**The Principle of Distinction**

Parties to an armed conflict, including in the cyber context, must at all times distinguish between civilians and combatants, as well as civilian objects and military objectives. IHL prohibits attacks that are not directed at a specific military objective, employ a method or means of combat which cannot be directed at a specific military objective, or employ a method or means of combat of a nature to strike military objectives and civilians or civilian objects without distinction.

In this context, in Austria’s view, civilian data are to be considered an “object” for the rules governing the conduct of hostilities and are protected under the principle of distinction. Similarly, ICT equipment and services of medical facilities and humanitarian relief organizations must be respected and protected. A cyber activity that deletes or manipulates data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations, is prohibited.

In the conduct of military operations, which may include cyber activities, the parties to an armed conflict are under an obligation to take constant care to spare the civilian population, civilians and civilian objects.

Civilians who directly participate in hostilities lose their protection against attack. In the cyber context, direct participation in hostilities commences with the first cyber activity launched and continues throughout the period of intermittent activity, resulting in the individual being a lawful target for the entire period of cyber activities conducted.

Generally, it is technically possible to direct cyber activities only against military objectives. If a target consists both of military and civilian components, an attack must – if feasible – always be directed only against the military parts of that target. In order to minimize the risks to civilians, parties to the conflict must – wherever feasible – only employ malware capable of discriminating between civilian objects and military objectives.
Some dual-use objects, such as means of communications or satellites, could, under certain circumstances, be categorized as military objectives, provided they make an effective contribution to military action and their destruction offers a military advantage. However, the fact that a dual-use object is a military objective does not automatically render every attack directed against it lawful. Stopping or impairing the civilian use of an object in violation of core IHL principles renders the attack unlawful despite the object’s classification as a military objective.

Nevertheless, even if a dual-use object, e.g. a communication system, were categorized as a civilian object, not every interference with it would be considered an unlawful attack. For instance, neither the jamming of radio communications nor of television broadcasts is considered an attack under IHL.

**Example 1:** In order to cause civil unrest in connection with an armed conflict, state A conducts a cyber activity solely designed to disrupt the internet services for the civilian population in the territory of state B. Such an activity is prohibited.

**Example 2:** State A conducts a cyber activity in connection with an armed conflict which disrupts a civilian internet service on which large parts of the civilian population in state B and some combatants rely. Such an activity is also prohibited.

**The Principle of Proportionality**

Attacks that are expected to cause incidental civilian harm, that is excessive in relation to the anticipated concrete and direct military advantage given the circumstances prevailing at the time, are prohibited. Attacks conducted through cyber means are capable of causing incidental civilian harm both during transit through other states and as a result of an attack itself.

When assessing incidental civilian harm, possible non-kinetic effects of an attack, such as the temporary deprivation of functionality of an ICT system, and possible indirect effects, need to be considered. Unexpected or unforeseeable harm to civilians or civilian objects is not to be considered in this assessment.

**e. Cyber Means of Warfare**

**Key Positions:**

It is prohibited to employ cyber means of warfare that are of a nature to cause superfluous injury or unnecessary suffering or are indiscriminate in nature.

All states are required to ensure that the cyber means of warfare they acquire or use comply with IHL.
The term “means of warfare” encompasses cyber weapons and cyber weapon systems and includes any device, materiel, instrument, mechanism, equipment or software used, designed or intended to be used to conduct an attack through cyber means.

In the cyber context, states must conduct a legal review (Art. 36 Additional Protocol I) to assess whether the employment of new cyber weapons or cyber means or methods of warfare is prohibited by international law. As cyber military capabilities may be less standardized than kinetic weapons, these reviews should be conducted in light of the specific cyber environment in which the weapon will likely be used.

13. International Criminal Law

**Key Positions:**

- **International criminal law**, including the Rome Statute of the International Criminal Court (ICC), applies to cyber activities. The ICC may also hear cases relating to cyber activities.
- Cyber activities in violation of IHL may amount to war crimes, or other international crimes, and, thus, give rise to individual criminal responsibility.

Cyber activities may amount to international crimes, i.e. genocide, crimes against humanity, war crimes, or the crime of aggression, when the actus reus and mens rea requirements are met.

Provided the criteria for jurisdiction under the Rome Statute are fulfilled, the International Criminal Court (ICC) is competent to decide cases against individuals alleged to have committed crimes under the Rome Statute through cyber activities. While cyber activities are in principle capable of amounting to international crimes, in practice, most cyber activities will not reach this threshold.

All modes of liability foreseen under international criminal law apply in the cyber context. This includes direct and indirect perpetration, superior responsibility, ordering, aiding and abetting and inchoate crimes, amongst others.

---

14. Neutrality

**Key Positions:**
The rights and obligations of neutral states in case of a war between states under international law are applicable to cyber activities.
A neutral State has the obligation to prevent any infringements of its neutrality, including the use of its territory by one of the conflicting parties.
Conflicting parties are obliged to respect the territorial integrity of the neutral state. They may neither conduct conflict-related cyber activities from installations on the territory or under the exclusive control of the neutral state, nor use or take control of a neutral state’s ICT infrastructure in order to carry out such activities.

The law of neutrality is applicable to cyber activities. This also pertains to the obligation of conflicting parties not to exercise any belligerent rights by cyber means on a neutral state’s territory.

A neutral state is not required to forbid or restrict the conflicting parties’ use of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals on its territory. In particular, as cyber activities are generally routed through ICT infrastructure (including cables) of other states, a mere transmission of data packets through the territory of a neutral state by one of the parties to the conflict, does not constitute a violation of the law of neutrality, nor is the neutral state obligated to prevent such transmission.

However, conflicting parties are forbidden to a) erect on the territory of a neutral state a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea, and b) use any installation of this kind established by them before the war on the territory of a neutral state for purely military purposes, and which has not been opened for the service of public messages.

The neutral state has a duty to prevent and terminate a violation of its neutrality. As permanent knowledge about the use of its ICT infrastructure by other states would require excessive monitoring by the neutral state (and thus might cause human rights violations), this duty is subject to certain limits. However, this does not absolve a neutral state from preventing and terminating any cyber activities on its territory by parties to the conflict conducted in connection with an armed conflict, of which it has become or should have become aware (cf. Chapter 8 on Due Diligence). Given the difficulties regarding the cross-border nature of cyber activities, any assessment of a violation of the law of neutrality must be made on a case-by-case basis.

---

36 Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Article 8.
37 Ibid., Article 3.
In accordance with Art. 103 UN Charter, neutrality does not apply when the UN Security Council, acting under chapter VII of the UN Charter, decides certain measures to be taken in order to maintain or restore international peace and security. Moreover, the obligations of a neutral state under the laws of neutrality become inapplicable as soon as the neutral state becomes itself the victim of an armed attack.

While Austria is a permanently neutral state, as an EU member state, it is also subject to the obligations arising from the EU Common Foreign and Security Policy (CFSP).38 According to Art. 23j of the Austrian Federal Constitutional Act, Austria participates in the EU’s CFSP. This provision entails a partial derogation from Austria’s obligations as a permanently neutral state whenever the EU acts within the framework of the CFSP.

* * *

---

38 Austria is also bound by Art. 42 (7) of the Treaty on European Union (Mutual Assistance Clause) to aid and assist, by all the means in its power, in accordance with Art. 51 UN Charter, a member state having become the victim of armed aggression on its territory. In this case, Austria shall aid and assist the attacked member state, taking into consideration the specific character of its security and defence policy (so-called “Irish Clause”).