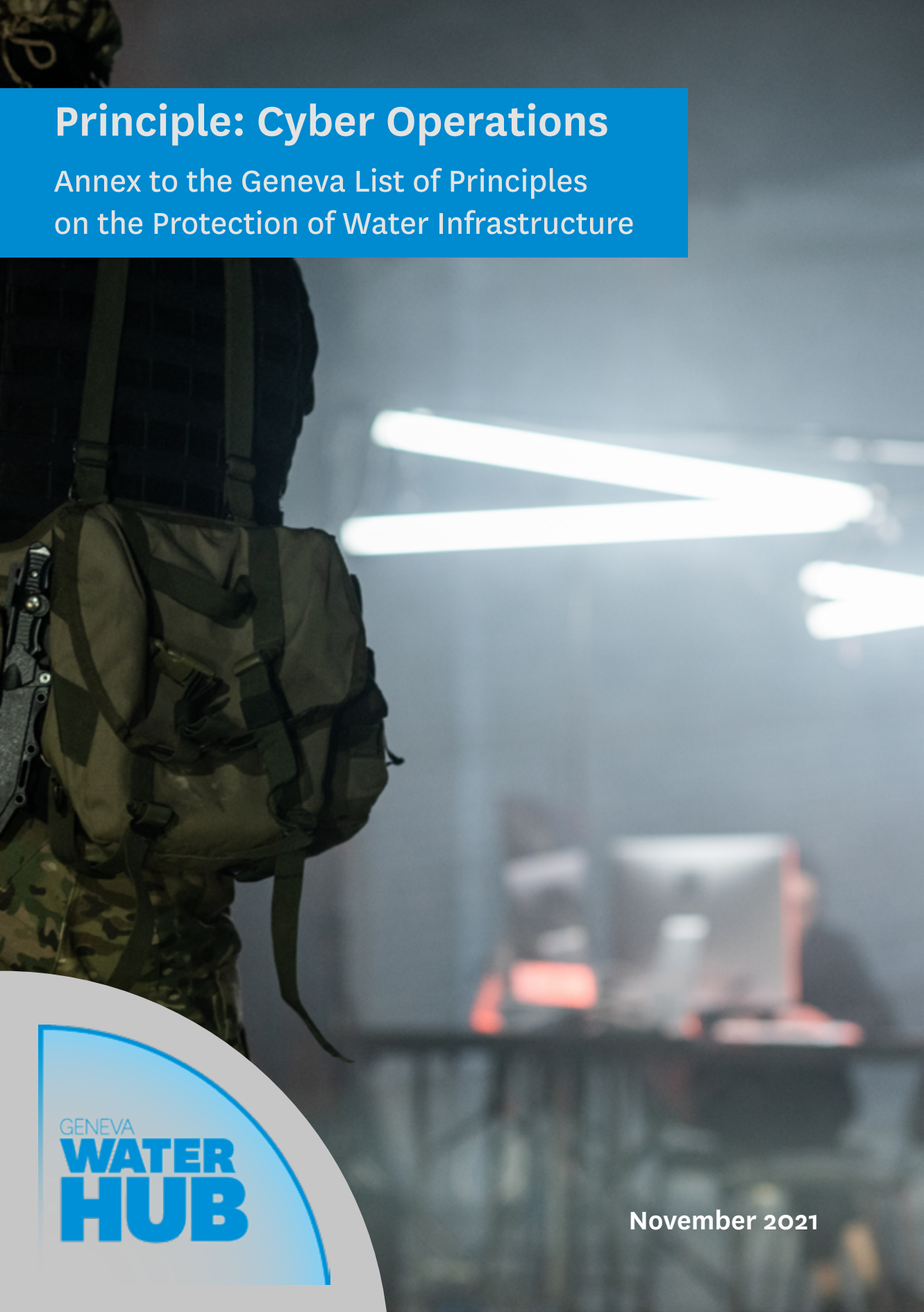
Principle: Cyber Operations

Annex to the Geneva List of Principles on the Protection of Water Infrastructure



GENEVA WATER HUB

November 2021

Photo credit
Rear view of two men in military uniform on Getty Images/iStockphoto

Principle: Cyber Operations

Annex to the Geneva List of Principles on the Protection of Water Infrastructure

November 2021

Introductory note

The advancement in technology and digitalization of the water sector has increased its vulnerability to cyberattacks that could contaminate, disrupt treatment and supply systems, or release dam waters. For instance, in February 2021, hackers broke into the city of Oldsmar's water treatment facility (in Florida) and changed chemical levels, making the water unsafe to consume.

Similarly, in 2020 Israel claimed that there were attempted cyberattacks against its water treatment plants and agricultural irrigation systems. These new typologies of attacks against water systems and infrastructure pose a real and significant risk to human life, the economy, and the security of states. Accordingly, there is a clear need to regulate threats emanating from such attacks.

In 2017, the Global High-Level Panel on Water and Peace, an initiative of fifteen countries, underscored the need to elaborate the international law rules protecting water infrastructures during armed conflicts. To that end, the Geneva Water Hub developed the Geneva List of Principles on the Protection of Water Infrastructure (Geneva List). The Geneva List systematizes the main rules applicable to the protection of water infrastructure during armed conflicts, specifically in the conduct of hostilities and post-conflict situations, and sets forth some recommendations that go beyond existing law.

In the context of armed conflict, international humanitarian law (IHL), which among other things, sets limits on the means and methods of warfare, be they kinetic or cyber, and protects civilians and civilian objects, including water infrastructure and water-related infrastructure. Thus, parties to armed conflicts must not disrupt the functioning of water infrastructure and water-related infrastructure through cyber operations. They must take all feasible precautions to avoid incidental harm to such facilities and related infrastructures.

However, in the Geneva List, there is no separate principle dedicated to cyber operations. Noting the emerging cyber security threats, evolution in military cyber capabilities, and the water sector's vulnerability, Geneva Water Hub developed a principle on 'Cyber Operations' dealing with the protection of water infrastructure

and water-related infrastructure. The principle mainly transposes the existing IHL rules and principles concerning the conduct of hostilities to this new domain. The principle also indicates that other branches of international law, such as human rights law, could provide protection.

In June 2021, the Geneva Water Hub and the Geneva Academy of International Humanitarian Law and Human Rights jointly organized a workshop on **'Cyber operations and the protection of water.'** The workshop took stock of international law practice on cyber security and focused on how the law applicable to cyber operations interacts with water and water-related infrastructure protection. The principle, with its commentary, was discussed during the workshop, and inputs from the International Committee of the Red Cross (ICRC), cyber security practitioners, military advisors and academic experts were incorporated. The Geneva Water Hub takes this opportunity to express its gratitude to all the workshop participants for their invaluable contributions.

Principle: Cyber Operations

1. Water infrastructure and water-related infrastructure must not be attacked, including when using cyber means and methods of warfare, unless they qualify as a military objective.

2. The parties to a conflict must not employ cyber means and methods of warfare:

(a) to attack, destroy, remove or render useless water infrastructure indispensable to the survival of the population, such as drinking water installations and supplies and irrigation work; and

(b) to attack water infrastructure containing dangerous forces, namely dams and dykes, even when these are military objectives, and other military objectives located at or in their vicinity, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.

3. During cyber operations, water infrastructure and water-related infrastructure should not be made the object of attack, even when these are military objectives, if such an attack is intended, or may be expected, to cause significant damage to the environment.

4. Cyber operations against water infrastructure and water-related infrastructure must also respect all other applicable international law rules identified under the Geneva List.

Commentary

1. The use of "cyber operations"[1] as means or methods of warfare in an armed conflict poses a real risk of harm to civilians and critical infrastructure. Developed with the traditional kinetic warfare in mind, international humanitarian law does not contain specific rules regulating cyber operations. However, its rules and fundamental principles apply to cyber operations conducted in the context of an armed conflict (international armed conflict and non-international armed conflict).[2] Notably, Additional Protocol lays down an obligation to carry out legal reviews of new weapons, means and methods of warfare,[3] which extends to military cyber capabilities intended for the use or expected to be used in the conduct of hostilities.[4] According to the International Court of Justice, international humanitarian law regulates "all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future."[5] Besides, the International Committee of the Red Cross asserts that international humanitarian law limits cyber operations during armed conflicts just as it limits the use of any other weapon, means and methods of warfare in an armed conflict.[6] Many states have agreed that if armed conflicts extend to cyberspace, international humanitarian law and, as appropriate other rules of international law will apply to such operations.[7] Such acceptance by states is vital as an increasing number of states are developing cyber capabilities for their armies, and their use is likely to increase in the future. According to the International Committee of the Red Cross, states' interpretation of existing international humanitarian law rules will determine the extent to which this area of international law protects against the effects of cyber operations.

[1] Similar to the definition used by the ICRC, the term 'cyber operations' is used to describe operations against a computer, a computer system or network, or another connected device, through a data stream, when used as means and methods of warfare in the context of an armed conflict. See ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts,' *ICRC position paper,* submitted to the 'Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security' and the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,' November 2019, (fn.1). The US DoD Manual defines Cyberspace Operations as operations that involve 'the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace.' See The US DoD Manual (2016), § 16.1.2.

[2] See ICRC *position paper* 2019, 4; and NATO Cooperative Cyber Defence Centre of Excellence (Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, Cambridge 2017), Commentary to Rule 80, § 1.

[3] Additional Protocol I, Art.36.

[4] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*- Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, 2019, 35.

[5] See *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) 1996 ICJ Reports 226, § 86.

[6] See ICRC *Position Paper* 2019, above note 1; and ICRC Challenges Report 2019, above note 4, 26-28.

[7] See The proposal by the High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - *Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013, 2013, 1 final.

However, according to the International Committee of the Red Cross, states should interpret international humanitarian law so as to preserve civilian infrastructure from significant disruption.[8] Moreover, to the extent that cyber activities against water infrastructure and water-related infrastructure conducted in the course of an armed conflict are not specifically addressed by existing rules of international humanitarian law, the Martens Clause,[9] which reflects customary international law,[10] provides that such infrastructure remains ''under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.''[11]

2. Cyber operations used as means and methods of warfare[12] in the context of an armed conflict, i.e., that either triggers an armed conflict or has a nexus to it, are governed by international humanitarian law. Cyber threats that are not conducted in relation to armed conflict but stem from economic or other espionage or organized cybercrime are not regulated by international humanitarian law. It is widely accepted that cyber operations that can be reasonably expected to cause death, injury, or physical damage constitute an ''attack'' under international humanitarian law.[13] In this view, the notion of attacks also encompasses cyber operations that ''disrupt essential services without necessarily causing physical damage constitute one of the most important risks for civilians'' and such an interpretation is in line with the object and purpose of the rules of international humanitarian law on the conduct of hostilities.[14] Moreover, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0) recommends that ''certain cyber operations, such as those affecting the delivery of humanitarian assistance should be governed by the IHL even if they do not rise tothe level of an 'attack.'''[15]

3. In the context of armed conflict, civilian infrastructure is protected against attacks, including using cyber means and methods of warfare, by existing

[8] ICRC *Position Paper* 2019, above note 1, 2.
[9] See Additional Protocol I, Art.1 (2); Additional Protocol II, Preamble, § 5; Hague Convention (II), Preamble, § 9; and Hague Convention (IV), Preamble, § 8.
[10] See Nuclear Weapons Advisory Opinion, above note 5, § 84.
[11] See Principle 23 on Martens Clause; and Tallinn Manual 2.0, above note 2, Commentary to Rule 80, §§ 11-12.
[12] As defined under Tallinn Manual 2.0, above note 2, Rule 103: 'means of cyber warfare' are cyber weapons and their associated cyber systems, and 'methods of cyber warfare' are the cyber tactics, techniques, and procedures by which hostilities are conducted.
[13] ICRC *Position Paper* 2019, above note 1, 7; and Tallinn Manual 2.0, above note 2, Rule 92.
[14] ICRC *Position Paper* 2019, above note 1, 7-8.
[15] Tallinn Manual 2.0, above note 2, Commentary to Rule 80, § 4.

fundamental rules and principles of international humanitarian law, particularly the principles of distinction, proportionality, and precautions in attack. Thus, even when water infrastructure and water-related infrastructure become military objectives, the principles of distinction, proportionality, and precautions, as reaffirmed by Principles 6, 7, 8, 9, 10, and 11 of the Geneva List, which apply to both international and non-international armed conflicts, must be respected. The principle of distinction requires that cyber operations must not be directed against civilians or civilian objects.[16] International humanitarian law prohibits attacks that are not directed at a specific military objective (e.g., attacks that treat as a single target a number of clearly discrete military objectives) and employing means and methods of warfare that cannot be directed at a specific military objective or the effects of which cannot be limited as required by law.[17] Thus, whenever parties to a conflict resort to cyber operations, they should respect the principle of distinction and avoid using cyber tools that spread and cause damage indiscriminately (including cyber capabilities that are by nature indiscriminate).

4. A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.[18] When water infrastructure and water-related infrastructure become military objectives, ''those who plan or decide upon an attack must do everything feasible to cancel or suspend it if it becomes apparent that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to theconcrete and direct military advantage anticipated.''[19] Similar to what is enshrined under paragraph 3 of Principle 9 of the Geneva List, the ICRC takes the view that the assessment of ''incidental civilian harm'' includes harm due to the foreseeable direct and indirect (or reverberating) effects of cyber operations.[20]

[16] Additional Protocol I, Arts.48, 51(2) and 52(2); Additional Protocol II, Art.13 (2); ICRC Customary IHL Study, Rules 1 and 7; Tallinn Manual 2.0, above note 2, Rule 93; and Principle 6 on attacks against water infrastructure and water-related infrastructure, and Principle 7 on attacks against the personnel.

[17] Additional Protocol I, Art.51 (4); ICRC Customary IHL Study, Rules 11 and 12; Tallinn Manual 2.0, above note 2, Rules 111-112; and Principle 8 on indiscriminate attacks.

[18] Additional Protocol I, Arts.51 (5) (b) and 57 (2) (a) (iii); ICRC Customary IHL Study, Rule 14; Tallinn Manual 2.0, above note 2, Rule 113; and Principle 9 on proportionality in attack.

[19] See Additional Protocol I, Art.57 (2) (b); and ICRC Customary IHL Study, Rule 19.

[20] ICRC *Position Paper* 2019, above note 1, 7.

5. Water infrastructure and water-related infrastructure are civilian objects and, hence, both precaution in cyber attacks and precaution against the effects of cyber attacks apply to their protection.[21] The responsibility to take precautionary measures by those taking offensive action and those whose networks and systems were at risk of being attacked is also reflected in the norms of responsible state behaviour in cyberspace adopted by the UN.[22] Thus, during military operations, including when using cyber means and methods of warfare, constant care must be taken to spare the civilian population and civilian objects;[23] those who plan or decide upon attack must do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection,[24] and in the choice of means and methods of attack to avoid or at least minimize, incidental loss of civilian life, injury to civilians and damage to civilian objects.[25] The International Committee of the Red Cross also underscores that when using cyber means or methods of warfare, parties to a conflict must take constant care to spare the civilian population and civilian objects to avoid or at least reduce incidental harm.[26] Besides, parties to the conflict must take all feasible precautions to protect the civilian population and civilian objects under their control against the effects of attacks.[27] Such measures, among others, could include reducing cyber vulnerabilities, isolating the military from civilian cyber infrastructure and networks, segregating computer systems on which essential civilian infrastructure depends from the internet, and work on the identification in cyberspace of the cyber infrastructure and networks serving protected objects (digitally marking protectedobjects).[28] Congruent with this, parties to the conflict are encouraged to isolate or digitally mark cyber infrastructure on which essential civilian infrastructure depends, including water infrastructure and water-related infrastructure.

---

[21] See Principle 10 on precautions in attack, and Principle 11 on precautions against the effects of attacks; and ICRC, *Avoiding Civilian Harm From Military Cyber Operations During Armed Conflicts*, Report prepared by Ewan Lawson and Kubo Mačák, ICRC *Expert Meeting*, Geneva, 21–22 January 2020, 25-31 & 54.

[22] UN General Assembly, 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, § 13 (f) & (g).

[23] See Additional Protocol I, Art.57 (1); ICRC Customary IHL Study, Rule 15; Tallinn Manual 2.0, above note 2, Rule 114; and ICRC *Position Paper* 2019, above note 1, 6.

[24] See Additional Protocol I, Art.57 (1) (a); ICRC Customary IHL Study, Rule 16; Tallinn Manual 2.0, above note 2, Rule 115; and Principle 10 on precautions in attack.

[25] See Additional Protocol I, Art.57 (2) (a); ICRC Customary IHL Study, Rule 17; Tallinn Manual 2.0, above note 2, Rules 116; and Principles 10 on precautions in attack.

[26] ICRC *Position Paper* 2019, above note 1, 5-6

[27] See Additional Protocol I, Art.58 (c); ICRC Customary IHL Study, Rule 22; Tallinn Manual 2.0, above note 2, Rule 121; and Principle 11 on precautions against the effects of attacks.

[28] ICRC *Position Paper* 2019, above note 1, 6; and ICRC *Expert Meeting Report* 2020, above note 21, 27-28 &54.

6. Under international humanitarian law, in addition to general protection, there are some objects, installations and areas specifically protected during the conduct of hostilities. Such protection is not limited to the use of kinetic means but covers all means and methods of warfare, including cyber operations, particularly considering their potential human cost.[29] Among such specific protections, the Geneva List includes three rules relevant for protecting water infrastructure and water-related infrastructure, namely objects indispensable to the survival of the population, works and installations containing dangerous forces, and protection of the environment.

7. Objects indispensable to the survival of the population benefit from specific protection under international humanitarian law. It prohibits attacking, destroying, removing or rendering useless objects indispensable to the survival of the population, such as drinking water installations and supplies and irrigation work.[30] Accordingly, parties to the conflict must not attack, destroy, remove or render useless water infrastructure indispensable to the survival of the civilian population.[31] It is evident that cyber operations against water treatment facilities to contaminate drinking water or disrupt distribution systems adversely affect water quality and supply, leading to supply shortages, which might also cause the spread of waterborne diseases, leading to a public health crisis.[32] Thus, such prohibitions are applicable, including when cyber means and methods of warfare are employed against water infrastructure.[33] Additionally, water infrastructure can be rendered useless by targeting water-related infrastructures that are necessary to their functioning (for example, as their power source), such as electricity-generating facilities. In such cases, the prohibition should be understood as also covering water-related infrastructure.

8. Works and installations containing dangerous forces and other military objectives located at or in their vicinity are also granted specific protection. Under customary international humanitarian law, it is established that particular care must be taken if works and installations containing dangerous forces, and other

[29] ICRC, *The Potential Human Cost of Cyber Operations*, Report prepared by Laurent Gisel and Lukasz Olejnik, ICRC *Expert Meeting* Geneva, 14 -16 November 2018, 73-74; & ICRC *Position Paper* 2019, above note 1, 5.
[30] See Additional Protocol I, Art.54 (2); Additional protocol II, Art.14; ICRC Customary IHL Study, Rule 54.
[31] Principle 12 on starvation and water infrastructure indispensable to the civilian population.
[32] ICRC *Expert Meeting* 2018, above note 29, 63; Madrid Rules, Art.1; Berlin Rules, Commentary to Art.50, 'Civilians are entitled to an adequate water supply under all circumstances. Hence the prohibition of any action, whatever the motive, which would have the effect of denying the civilian population of the necessary water supply.'
[33] See Tallinn Manual 2.0, above note 2, Rule 141; ICRC *Expert Meeting* 2018, above note 29, 73.

installations located at or in their vicinity are attacked, in order to avoid the release of dangerous forces and consequent severe losses among the civilian population.[34] State parties to Additional Protocol I are prohibited to attack works or installations containing dangerous forces, even where these objects are military objectives, and other military objectives located at or in their vicinity, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population, subject to the exceptions of Article 56(2).[35] For non-international armed conflict, Additional Protocol II stipulates a similar prohibition under Article 15 but did not include the exceptions mentioned under Article 56 (2). Thus, water infrastructure containing dangerous forces, namely dams and dykes, even when these are military objectives, and other military objectives located at or in their vicinity, must not be made the object of attack if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.[36] The prohibition equally applies to cases where parties to armed conflict employ cyber means and methods of warfare.[37] Parties to the conflict are encouraged to extend the prohibition to use cyber means and methods of warfare against dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity to all water infrastructure containing dangerous forces such as water treatment plants, and water-related infrastructure they depend on.

9. International humanitarian law also specifically prohibits the use of means and methods of warfare that are intended or may be expected to cause widespread, long-term and severe damage to the natural environment.[38] Concerning the use of cyber means and methods against the natural environment, Tallinn Manual 2.0 underlines that ''the natural environment is a civilian object and as such enjoys general protection from cyber attacks and their effects'' and that employing cyber means and methods of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment isprohibited.[39] Water resources are part of the natural environment and benefit from such protection. Besides, water treatment plants and pumping stations may have

[34] ICRC Customary IHL Study, Rule 42.
[35] Additional Protocol I, Article 56.
[36] Principle 13 on water infrastructure containing dangerous forces.
[37] See Tallinn Manual 2.0, above note 2, Rule 140.
[38] See Additional Protocol I, Arts.35 (3) and 55 (1); and ICRC Customary IHL Study, Rule 45. See also, International Law Commission, Protection of the environment in relation to armed conflicts: Text of the draft principles provisionally adopted during the present session by the Drafting Committee, A/CN.4/L.937 (6 June 2019), Principle 13; and ICRC, Guidelines on the Protection of the Natural Environment in Armed Conflict: Rules and Recommendations Relating to the Protection of the Natural Environment under International Humanitarian Law, with Commentary, 2020, Rule 2.
[39] Tallinn Manual 2.0, above note 2, Rule 143; and ICRC *Expert Meeting* 2018, above note 29, 73

reserves of toxic industrial chemicals, and attacking them (e.g., use cyber means to trigger a release of oil into a waterway) might have significant adverse effects on the environment. To that end, the Geneva List provides that water infrastructure and water-related infrastructure should not be made the object of attack, even when these are military objectives, if such attack is intended, or may be expected, to cause significant damage to the environment.[40] Thus, cyber operations must be employed with due regard to protecting and preserving the environment, including water infrastructure and water-related infrastructure.

10. As enshrined under paragraph 4, in addition to the protections reaffirmed under paragraphs (1), (2) and (3), there are other relevant rules identified by the Geneva List applicable to the protection of water infrastructure in the context of armed conflict as well as in post-conflict situations. They include some specific protections and prohibitions under international humanitarian law, human rights law, and international water law. For example, international humanitarian law prohibits acts or threats of violence the primary purpose of which is to spread terror among the civilian population.[41] Such conduct is prohibited, including whencarried out through cyber means or methods of warfare.[42] Similarly, as the use of poison or poisoned weapons is prohibited, cyber means or methods of warfare must not be employed to poison water.[43] Besides, international humanitaria law prohibits forced displacement of the civilian population.[44] Accordingly, cyber operations towards water infrastructure, such as control over water supply, release (flooding) or deprivation, must not be used to force the displacement of civilians.[45] Moreover, parties to an armed conflict have a duty not to hamper the necessary humanitarian access and assistance.[46] As underscored by the Tallinn Manual 2.0, ‘‘cyber operations shall not be designed or conducted to interfere unduly with impartial efforts to provide humanitarian assistance’’[47] Furthermore, in the situation of occupation, the Occupying Power has an obligation to restore and ensure public order and safety (encompassing restoring and ensuring civil life)[48] and ensure

[40] See Principle 15 on the protection of the environment.
[41] Additional Protocol I, Art.51 (2); Additional protocol II, Art.13 (2); ICRC Customary IHL Study, Rule 2.
[42] See Tallinn Manual 2.0, above note 2, Rule 98; and Principle 14 on acts or threats of violence the primary purpose of which is to spread terror among the civilian population.
[43] See Hague Convention II), Art.23 (a); ICRC Customary IHL Study, Rule 72; and Principle 5 on poison or poisoned weapons.
[44] See Geneva Convention IV, Art.49; Additional Protocol II, Art.17; and ICRC Customary IHL Study, Rule 129.
[45] See Principle 16 on forced displacement.
[46] See Geneva Convention IV, Art.23; Additional Protocol I, Art.70; Additional Protocol II, Art.18 (2); ICRC Customary IHL Study, Rule55; and Principle 17 on humanitarian access and assistance.
[47] Tallinn Manual 2.0, above note 2, Rule 145.
[48] See Hague Regulations, Art.43. See also, ICRC, *Occupation and Other Forms of Administration of Foreign Territory*, Report (2012), 56-58.

that the population under its control has necessary foodstuffs and other supplies essential to its survival.[49] Such obligations entail, among other things, restoring and maintaining cyber infrastructure that is essential to ensure water treatment and supply network.[50]

11. As enshrined under Principle 1 (2) and (3), the Geneva List is intended for both international armed conflict and non-international armed conflicts and addressed to both states and non-state actors. Accordingly, during non-international armed conflict, all parties involved are obligated to respect the relevant IHL rules applicable to cyber operations.

12. The Geneva List also identified other relevant rules from other branches of international law that govern and provide protection to water infrastructure and water-related infrastructure. These rules are vital concerning cyber activities that neither trigger an armed conflict nor have nexus to it but impacting such infrastructures. For instance, international human rights law, which applies in peacetime and continues to apply in armed conflict,[51] recognizes that everyone has the rights to water and sanitation as components of the right to an adequate standard of living and as being indispensable for the full enjoyment of all human rights, including the right to life.[52] The Tallinn Manual 2.0 recognized that international human rights law (both treaty and customary law) applies to ''cyber-related activities,'' including in the context of an armed conflict, and imposes the obligation to respect and protect human rights.[53] Similarly, the Geneva List restates the importance of the human rights to water and sanitation for the full enjoyment of all human rights and reaffirms the obligation to ensuring access to sufficient, safe, acceptable, physically accessible and affordable water, and physical and affordable access to sanitation.[54] Consequently, cyber operations that interfere with water treatment or supply systems or generally impact water infrastructure and water-related infrastructure could violate human rights, including the rights to water and sanitation, the right to life and the right to health.

[49] Geneva Convention IV, Arts.55-56; and Additional Protocol I, Art.69 (1).
[50] Tallinn Manual 2.0, above note 2, Commentary to Rule 147, § 2.
[51] See Nuclear Weapons Advisory Opinion, above note 5, § 25; and *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion) 2005 ICJ Reports 13, § 106.
[52] See also UN Committee on Economic, Social and Cultural Rights, *General Comment No.15: The right to water (Arts. 11 and 12 of the Covenant)* (2003), § 3; Convention on the Elimination of All Forms of Discrimination Against Women (18 December 1979), Art.14 (2) (h); Convention on the Rights of the Child (20 November 1989), Art.24 (2) (c) and (e); Convention on the Rights of Persons with Disabilities (13 December 2006), Art.28 (2) (a); UNHRC Res 15/9 (6 October 2010), § 3; UNGA Res 70/169 (17 December 2015), § 7.
[53] See Tallinn Manual 2.0, above note 2, Rules 34 - 36.
[54] See Principle 3 on the human rights to water and sanitation with its commentary.

13. It is generally accepted that states assume extraterritorial human rights obligations to those within their ''power or effective control,''[55] regardless of the circumstances in which such power or effective control was obtained.[56] Regarding extraterritorial human rights obligation for cyber activities, the Tallinn Manual 2.0 mentions that there is some disagreement over whether human rights treaty obligations apply extraterritorially but affirms that customary international human rights law applies extraterritorially in situations where a state exercises ''power or effective control,'' as it does offline (when a state exercises physical control over territory or persons).[57] The Tallinn Manual 2.0, however, acknowledges that there is no consensus among experts on whether state measures that do not involve an exercise of physical control (activities conducted through cyberspace only) may qualify as ''power or effective control.''[58] When states exercise power or effective control extraterritorially, they must refrain from acts that might unduly interfere with the enjoyment of the human rights to water and sanitation, including limiting access to, or destroying, water services and infrastructure.[59] Such negative obligation to respect the rights to water and sanitation applies extraterritorially, as states are under obligation to respect the enjoyment of the right in other countries and also international cooperation requires states to ''refrain from actions that interfere, directly or indirectly, with the enjoyment of the right to water in other countries.''[60] Additionally, a state should have an obligation for extraterritorial harm if it controls cyber infrastructure or the infrastructure from where the cyber operation is launched is in its territory.

14. International water law likewise provides some protection to water resources in the context of cyber operations. For instance, the Convention on the Law of the Non-Navigational Uses of International Watercourses (UN Watercourses Convention) stipulates that 'international watercourses and related installations,

[55] The UN Human Rights Committee elaborated the notion of exercise of power or effective control under it General Comment 36, Article 6 (Right to Life). It illustrates that 'State party has an obligation to respect and to ensure the rights under article 6 of all persons who are within its territory and all persons subject to its jurisdiction, that is, all persons over whose enjoyment of the right to life it exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner.' See UN Human Rights Committee, *General comment no. 36, Article 6 (Right to Life)* (2019), § 63.

[56] UN Human Rights Committee, General Comment No.31: *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, (2004), CCPR/C/21/Rev.1/Add.13, §10; ICJ, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004, §§ 107-112; and *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* (Judgment) 2005 ICJ Reports 168, §§ 216-217.

[57] See Tallinn Manual 2.0, above note 2, Commentary to Rule 34, §§ 1-7.

[58] *Ibid.*, Commentary to Rule 34, §§ 8-11.

[59] See General Comment No.15, above note 52, § 21.

[60] *Ibid.*, § 31.

facilities and other works shall enjoy the protection accorded by the principles and rules of international law applicable in international and non-international armed conflict.'[61] As indicated above, these protections of international humanitarian law equally apply when parties to an armed conflict use cyber means or methods of warfare, and this is vital in the face of the ever-increasing digitalization of the water sector and the management of transboundary watercourses. International water law also imposes the obligation not to cause transboundary harm, such as poisoning that has transboundary effects.[62] Likewise, the principle of equitable and reasonable utilization of shared watercourses requires the sustainable use of water and the protection of ecosystems.[63] States that share transboundary watercourses have an obligation to "employ their best efforts to maintain and protect installations, facilities and other works related to an international watercourse"[64] including taking all reasonable precautions to protect such works from foreseeable damages. Moreover, watercourse states should cooperate, even during situations of armed conflict, including the exchange of data and information, notification, communication, consultations and negotiations.[65] Furthermore, watercourse states should create joint mechanisms and commissions to ensure the protection, safe operation and maintenance of water infrastructure on transboundary water resources.[66] Accordingly, in the protection and use of transboundary watercourses, cyber activities of states, both during and outside the context of armed conflict, should be conducted in compliance with these obligations.

15. Finally, critical infrastructures, such as water and sewage supply systems, are particularly vulnerable to malicious cyber attacks from other states or non-state actors. Under international law, states have a due diligence obligation not to knowingly allow their territory to be used for internationally wrongful acts against another state,[67] which is equally relevant for activities in cyberspace. The UN established an Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications, and the latter's report underscores that "States should not conduct or knowingly support ICT activity contrary to their

[61] See UN Watercourses Convention, Art.29.
[62] See UN Watercourses Convention, Art.7; and UNECE Convention), Art.2.
[63] See e.g., UN Watercourses Convention, Arts.5, 7 and 20; and UNECE Convention Arts.2 (1) and 2 (2).
[64] See UN Watercourses Convention, Art.26 (1).
[65] *Ibid*., Art.30-31.
[66] See UN Watercourses Convention, Arts.8 and 24 (1); UNECE Convention, Art.9 (2); and Principle 20 on joint mechanisms and commissions.
[67] See ICJ, *Corfu Channel (United Kingdom v. Albania)*, judgement, 9 April 1949, 22; and Trail Smelter Arbitration (US v. Canada), Arbitral Tribunal, 3 UN Rep. Int'l Arb. Awards 1905.

obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public. Furthermore, States should continue to strengthen measures to protect all critical infrastructure from ICT threats and increase exchanges on best practices with regard to critical infrastructure protection.''[68] Likewise, Tallinn Manual 2.0 has included the principle of due diligence and mentioned that ''a State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect therights of, and produce serious adverse consequences for, other states.''[69] It further stated that ''the principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.''[70] Nevertheless, as pointed out under the Tallinn Manual 2.0, there are some delicate issues regarding this principle.[71]

[68] UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, A/AC.290/2021/CRP.2, 10 March 2021, § 31.
[69] Tallinn Manual 2.0, above note 2, Rule 6.
[70] *Ibid.*, Rule 7.
[71] See e.g., *Ibid.*, Commentary to Rule 6, §§ 29-30; and Commentary to Rule 7, §§ 3-4 & 14-15.

The Geneva Water Hub

Secretariat of the Global High-Level Panel on Water and Peace