COSTA RICA's POSITION ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

Introduction

1. The advent and rapid development of information and communications technologies (ICTs) have brought both opportunities and challenges for the international community. On the one hand, the Internet and other ICTs have facilitated the exchange of information between different actors and improved the provision of public and private services in societies around the world. By cutting costs and physical barriers, digital connectivity has been an important enabler of economic development and human rights. This is especially true for vulnerable groups in developing countries, as women and LGBTQI+ people. At the same time, the pervasiveness of and societal dependence on these technologies has increased our vulnerability to their use for malicious purposes by both State and non-State actors. Malicious cyber operations have targeted different components of ICTs, namely, software, hardware and data, as well as the human beings using or otherwise affected by these technologies.

2. During the COVID-19 pandemic, social distancing forced societies to move most of their public and private activities online. This led to a proliferation of harmful cyber operations. Examples ranged from disruptive cyber operations targeting the healthcare sector, including hospitals and research institutions, to disinformation campaigns on medical treatments and other measures to curb infection rates. Elections and other democratic processes have also reportedly been the subject of recurring interference by cyber means in numerous States.

3. Furthermore, ransomware has emerged as one of the most pressing cyber threats against national stability as well as international peace and security. Whether employed as a commercial service or for political purposes, ransomware can cripple the operations of private entities and entire governmental organs. This may have significant economic, political, and human costs, as the ransomware attacks targeting Costa Rica in 2022 illustrates. The theft and encryption of confidential governmental and personal data, coupled with demands for ransom payment and changes in Costa Rica's sovereign policy decisions have led to unprecedented disruptions to our finance, social security, healthcare, and other sectors. The long-term impact on those sectors is still felt. Costa Rica also notes with great concern the dangers arising from the deployment of military cyber capabilities during an ongoing armed conflict, including the risk of spillover effects on neutral States.

4. Many such operations have targeted or threatened critical infrastructure, such as the financial, healthcare, energy, water and sanitation sectors. While the definition of critical infrastructure varies among States, their vital importance calls for increased protection. In Costa Rica's view, it is also imperative not to lose sight of the gendered impact of cyber operations. Women, girls, persons with disabilities; LGBTQI+ people; migrants, refugees, and asylum seekers; older persons; and other vulnerable groups may be especially targeted by malicious uses of ICTs, including cyber surveillance, doxing, online harassment and hate speech. Likewise,

Costa Rica notes that access to and knowledge of ICTs is still unequal among different genders and societal groups.

5. It is against this backdrop that Costa Rica presents its national position on how international law applies to cyber operations. This is based on our fundamental national security and foreign policy interest in fostering the development of secure, resilient, and human-centric digital infrastructures on the basis of our core interests in protecting individuals and organizations at risk, with a strong emphasis on privacy and digital rights; defending citizens against threats to their freedom and dignity; promoting respect for human rights; and upholding democratic principles and the rule of law. In doing so, it encourages other States to issue their own national positions to foster greater transparency, clarity, and agreement around the existing international legal framework applicable to ICTs. Costa Rica also stresses the importance of United Nations (UN) processes dedicated to the discussion of this issue, namely the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG), as well as those under the auspices of the Organization of American States (OAS), such as the initiatives of the Inter-American Juridical Committee. In particular, it notes the contribution of such processes – all of which Costa Rica has participated in – to the clarification of how several rules of international law apply to cyber operations.[1] Moreover, Costa Rica notes the importance of capacity-building and dialogue on how international law applies to ICTs to enable and empower different States, particularly developing countries, to express their informed views on the subject.[2]

6. In the preparation of its statement, Costa Rica benefited from reflecting on the views of a wide range of States and other stakeholders including the International Committee of the Red Cross,[3] and it was guided by academic projects on the application of international law to cyber operations, such as the Tallinn Manual, the Oxford Process, and the Cyber Law Toolkit.[4]

[1] E.g., GGE, '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 ('GGE 2015 Report'), paras 24-29; 'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', A/76/135, 14 July 2021 ('GGE 2021 Report'), paras 69-73; OEWG, 'Final Substantive Report', 10 March 2021, A/AC.290/2021/CRP.2 ('OEWG Final Substantive Report'), paras 34-37; OEWG 'Annual Progress Report', A/77/275, 8 August 2022 ('OEWG 2022 Annual Progress Report'), Annex, para. 15; OAS, 'Report of the Inter-American Juridical Committee: International Law Applicable to Cyberspace', 24 August 2022, CJI/doc. 671/22 rev.2, 24 August 2022, pp. 11-22.

[2] GGE 2021 Report (n 1), para. 89(e); OEWG Final Substantive Report (n 1), para. 39; OEWG 2022 Annual Progress Report (n 1), para. 15(d).

[3] See ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, Position Paper, 2019.

[4] See M. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017) ('Tallinn Manual 2.0'); University of Oxford, *The Oxford Process on International Law Protections in Cyberspace: A Compendium* (2022), available at: https://www.elac.ox.ac.uk/wp-content/uploads/2022/10/Oxford-Process-Compendium-Digital.pdf; *Cyber Law Toolkit*, available at: https://cyberlaw.ccdcoe.org/.

The application of international law in cyberspace

7. Costa Rica believes that **existing international law applies in its entirety to ICTs, just as it does to all other technologies**.[5] With regard to the prohibition on the use of force and the rules of international humanitarian law, the International Court of Justice (ICJ) has held that these rules apply 'to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future'.[6] The same logic applies to the entirety of international law: as a matter of principle, it is applicable to all forms of human activity, whether they involve new technologies or not.

8. Existing international law applies to and governs the use of ICTs by State and non-State actors. Cyber-specific State practice and *opinio juris* can be useful in fleshing out how international law applies to ICTs and may eventually develop the law in this context. In the same vein, the non-binding, voluntary norms of responsible State behavior in cyberspace, articulated by the GGE and OEWG, do not replace, but are complementary to existing international law in the cyber context.[7]

9. Accordingly, it is emphasized the relevance of strengthening and improvement of international cooperation guided by international law in cyberspace, as a global public good.

State responsibility

10. Costa Rica believes that, under customary international law, as codified in Articles 1 and 2 of the International Law Commission (ILC)'s Articles on Responsibility of States for Internationally Wrongful Acts ('the ILC Articles'),[8] **cyber operations may amount to internationally wrongful acts engaging the responsibility of a State when they can be attributed to it and involve a breach of its international obligation(s)**.

11. In Costa Rica's view, **the existing customary thresholds for legal attribution of conduct to States continue to apply in cyberspace**.[9] Thus, cyber operations can only be attributed to a State when they are carried out by, *inter alia,* i) State organs,[10] including persons or groups under complete dependence on the State,[11] ii) persons or entities empowered by law to exercise elements of governmental authority,[12] including organs placed at the disposal of

[5] See, e.g., GGE 2015 Report (n 1), para. 24; OEWG Final Substantive Report (n 1), para. 34.
[6] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 ICJ 226 Rep ('*Nuclear Weapons case*'), paras 39, 85–86.
[7] OEWG Final Substantive Report (n 1), para. 25.
[8] ILC, 'Responsibility of States for Internationally Wrongful Acts', UNGA Res. 56/83, 12 December 2001, corrected by A/56/49(Vol. I)/Corr.4 ('ILC Articles').
[9] Articles 4-11, ILC Articles (n 8).
[10] Article 4, ILC Articles (n 8).
[11] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)*, Judgment, 1986 ICJ Reports 14 ('*Nicaragua case'*), paras 109–110.
[12] Article 5, ILC Articles (n 8).

States by other States,[13] iii) persons or groups acting on the instructions or under the direction or control of the State,[14] and iv) conduct acknowledged and adopted by the State as its own.[15]

12. **Legal attribution must be distinguished from the processes of technical and political attribution**. Technical attribution comprises a factual investigation into the source of a cyber operation. This often requires technical expertise and is fraught with challenges given cyberspace's decentralized nature and the widespread use of spoofing techniques and 'false flags'. Political attribution is the discretionary decision of a State to single out a certain entity, whether a State or a non-State actor, as the author of a certain cyber operation. While international law neither imposes a specific evidentiary threshold for legal attribution nor requires the publication of any evidence for this purpose,[16] States should consider all relevant information when legally attributing cyber operations to another State, publicly or not.[17]

13. Pursuant to the customary rules of State responsibility, **States directly injured by cyber operations amounting to internationally wrongful acts may respond by resorting to cyber or non-cyber countermeasures**.[18] Cyber countermeasures may also be taken in response to non-cyber internationally wrongful acts. Countermeasures are the non-forcible suspension of an international obligation whose wrongfulness is precluded by the prior breach of international law.[19] They may be taken by an injured State only in order to induce the responsible State to comply with its international obligations of cessation and/or reparation of the wrongful conduct.[20] Countermeasures, online or offline, must not be punitive,[21] and they must be proportionate to the injury suffered, considering the gravity of the breach and the rights in question.[22] They may not affect the prohibition on the use of force and other peremptory rules of international law, fundamental human rights, rules of a humanitarian character prohibiting reprisals, binding dispute settlement procedures, as well as diplomatic and consular law.[23]

14. To avoid the risk of escalation into conflict, **countermeasures are subject to certain procedural conditions under customary international law.** These are the requirements of i) calling upon the responsible State to fulfill its obligations of cessation and/or reparation, ii) notification of the intention or decision to take countermeasures, and iii) offer to negotiate with the responsible State.[24] However, in Costa Rica's view and considering the above-mentioned

[13] Article 6, ILC Articles (n 8).
[14] Article 8, ILC Articles (n 8).
[15] Article 11, ILC Articles (n 8).
[16] *Tallinn Manual 2.0* (n 4), at 83, para. 13.
[17] GGE 2015 Report (n 1), paras 13(b) and 28(f).
[18] *Tallinn Manual 2.0* (n 4), Rule 20, at 111ff.
[19] Articles 22 and 49(2), ILC Articles (n 8).
[20] Article 49(1), ILC Articles (n 8).
[21] Article 49(1), ILC Articles (n 8).
[22] Article 51, ILC Articles (n 8).
[23] Article 50, ILC Articles (n 8).
[24] Article 52, ILC Articles (n 8).

conditions, the procedural requirements do not have to be met when compliance with them would defeat the purpose of the intended countermeasures.[25]

15. In Costa Rica's view, countermeasures may be taken by the injured State, i.e., the State specifically affected by the breach, as well as third States in response to violations of obligations of an *erga omnes* nature or upon request by the injured State.[26] Thus, **States may respond collectively to cyber or non-cyber operations that amount to internationally wrongful acts**, by resorting to cyber or non-cyber countermeasures. Countermeasures must be distinguished from acts of retorsion, i.e., unfriendly acts taken in response to lawful but equally unfriendly acts by another State, such as the suspension of diplomatic relations.[27] Measures of retorsion are also available in cyberspace, including in response to wrongful or unfriendly cyber operations.

16. Other circumstances precluding wrongfulness under customary international law which are also applicable in the context of cyber operations are consent, necessity, force majeure, and self-defense, addressed below.

Peaceful settlement of disputes

17. In accordance with Article 2(3) of the UN Charter, States 'shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered'. Likewise, under Article 33(1) of the Charter, in the case of a dispute 'the continuance of which is likely to endanger the maintenance of international peace and security', States 'shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.' They must do so in good faith.[28] **Both provisions encapsulate the customary principle of peaceful settlement of disputes,[29] which applies to factual or legal disputes involving cyber operations**.[30]

Sovereignty

18. Sovereignty is a fundamental principle of international law, underpinning the entire international legal order and firmly grounding the position of States therein. Sovereignty has been traditionally understood in a territorial and physical sense. It means, first and foremost, a State's right to exercise legislative, adjudicative, and enforcement jurisdiction in its territory,

[25] ILC, 'Fourth report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur', A/CN.4/444 and Add.1-3, 1992, para. 16.
[26] Articles 48 and 54, ILC Articles (n 8).
[27] Draft ILC Articles (n **Error! Bookmark not defined.**), Commentary to Chapter II, para. 3.
[28] *Tallinn Manual 2.0* (n 4), Rule 65, esp. para. 14, at 308.
[29] UN General Assembly (UNGA), 'Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations', A/RES/2625(XXV), 1970 ('Friendly Relations Declaration'), Preamble, lit 'b' and Principle II.
[30] *Tallinn Manual 2.0* (n 4), Rule 65.

as well as the power to regulate the conduct of certain persons and events abroad.[31] Sovereign rights also have corollary duties, in particular, the obligation of a State to respect other States' sovereign rights and protect them within its territory.[32]

19. **Sovereignty also applies to cyberspace, including its physical and non-physical components.** After all, in the digital age, a State's sovereign powers over its territory and other objects or subjects are increasingly exercised through and dependent on the use of ICTs. In Costa Rica's view, sovereignty **is also a self-standing right accompanied by a binding international legal obligation[33] that can be breached by both cyber and non-cyber activities**.[34]

20. **Such breaches may occur when cyber operations cause physical damage[35] or loss of functionality of cyber infrastructure located in the victim State, regardless of ownership**.[36] Examples range from personal computers to programmable logic controllers or industrial computers that control energy, water, and sanitation facilities. For Costa Rica, a loss of functionality of these devices may occur in two ways. First, when the cyber operation attributable to another State entails the need to **repair or replace physical components** of the targeted cyber infrastructure or compromises physical equipment reliant on such infrastructure.[37] Second, loss of functionality may occur if the operating system or database upon which the targeted cyber infrastructure relies **stops functioning as intended**, as may be the case, for instance, as a result of ransomware.[38]

21. **Breaches of sovereignty may also occur when a State engages in cyber operations that constitute a usurpation of inherently governmental functions**, irrespective of any physical or non-physical effects on hardware or software located in the territory of the victim State.[39] Examples of cyber operations amounting to this type of violation are those interfering with a State's democratic processes, such as elections, responses to a national security or health emergency, such as the COVID-19 pandemic, and its choice of foreign policy.

22. It is important to note that it is often difficult to technically distinguish between a mere data-gathering operation from an operation penetrating a governmental system in order to interfere with a State's sovereign functions. Real-world examples show that, once a piece of malware successfully enters a system or network, it remains a latent threat to its integrity. This may damage software or hardware and thus interfere with the conduct of State affairs. Furthermore, surveillance operations may be carried out in ways that lead to breaches of State

[31] *S.S. 'Lotus', France v Turkey*, Judgment No 9, PCIJ Series A No 10, ICGJ 248 (PCIJ 1927), (1935), paras 38-45.
[32] *Island of Palmas Case (or Miangas), United States v Netherlands*, Award, 4 April 1928, II RIAA 829 (1928), ICGJ 392 (PCA 1928), at 839.
[33] *Nicaragua case* (n 11), paras 15 and 292.
[34] *Tallinn Manual 2.0* (n 4), Rule 4, at 17ff.
[35] Ibid, at 18, para. 5.
[36] Ibid, at 21, para. 13.
[37] Ibid.
[38] Ibid, at 21, paras 13-14.
[39] Ibid, at 21-27, paras 15-32.

sovereignty or other rules of international law.[40] As such, Costa Rica believes that, in some circumstances, cyber espionage may amount to a breach of State sovereignty.

Non-intervention

23. **The principle of non-intervention is grounded in customary international law and prohibits States from interfering directly or indirectly with matters within the domestic jurisdiction of other States**, i.e., their internal or external affairs.[41] According to the ICJ, a prohibited intervention is one bearing 'on matters in which each State is permitted, by the principle of State sovereignty, to decide freely'.[42] Examples include 'the choice of a political, economic, social and cultural system, and the formulation of foreign policy',[43] whether these are carried out by private or public entities,[44] and irrespective of a State's new undertakings under international law. Moreover, according to the ICJ, a wrongful intervention is one which 'uses methods of coercion in regard to such choices, which must remain free ones'.[45]

24. Coercion is clear-cut when a State uses or threatens to use force against another one.[46] Nonetheless, it can also occur in a multitude of ways **where one State, directly or indirectly through support for non-State actors, deprives another State of the capacity to make free and informed choices pertaining to its internal or external affairs**.[47] Coercion may occur when a State provides financial or other forms of support to secessionist, subversive or violent groups in the territory of another State, when it exercises significant political or economic pressure on another State, or when it engages in or supports subversive or hostile propaganda or the dissemination of false news that interfere in the internal or external affairs of another State.[48] Moreover, coercion needs not be successful in intervening within a State's internal or external affairs. Mere threats of intervention or acts seeking to interfere within another State's *domaine reservé* may also breach the principle.[49] For such breaches to occur, it suffices that a State intends to coerce another State, employs coercive methods, or eventually causes coercive effects in another State.

25. **In Costa Rica's view, these various forms of coercion may well be carried out in or through ICTs and amount to violations of the principle of non-intervention insofar as they interfere with a State's internal or external affairs**.[50] A prominent example of a breach of non-intervention are ransomware attacks crippling or simply interfering with a State's ability

[40] 'The Oxford Process on International Law Protections in Cyberspace: A Compendium', Oxford Institute for Ethics, Law and Armed Conflict (ELAC), October 2022, at 280, para. 3.
[41] Friendly Relations Declaration (n 29), Preamble, lit c, and Principle III.
[42] *Nicaragua case* (n 11), para. 205
[43] Ibid.
[44] *Tallinn Manual 2.0* (n 4), Rule 66, especially paras 8-11, at 315-316.
[45] *Nicaragua case* (n 11), para. 205.
[46] Ibid.
[47] *Tallinn Manual 2.0* (n 4), Rule 66, paras 18, 23, at 317, 319-320.
[48] UNGA 'Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States' UN Doc A/RES/36/103 (1981), II.
[49] Ibid.
[50] *Tallinn Manual 2.0* (n 4), Rule 66.

to run public services, such as finance, education, and social security. Moreover, foreign election interference may also infringe the principle of non-intervention. This may take the form of cyber operations directly interfering with mail ballots or voter databases, or electoral disinformation campaigns seeking to mislead the electorate about the vote itself, candidates, electoral polls or results. Other types of disinformation, such as those affecting a State's health policies, may also amount to a prohibited intervention. Posts inciting individuals or other States to wage wars of aggression or to disrupt or subvert the internal order of another State may likewise breach the principle of non-intervention.

Due diligence

26. In international law, **'due diligence' refers to a flexible standard of reasonable care against which State conduct can be assessed**.[51] This standard is found in different rules and regimes of international law, both general and specific.[52] These rules usually require States to take action with a view to preventing, stopping or redressing different harms to certain protected persons or objects, irrespective of the author or source of the harmful act.[53]

27. Under customary international law, States have a general obligation '**not to allow knowingly its territory to be used for acts contrary to the rights of other States**'.[54] This duty is a corollary of State sovereignty and requires States to protect the rights of other States in their territory.[55] It may be breached when a State knows or should have known that an act contrary to the rights of another State originates or transits through its territory, and yet fails to take reasonable action to stop or prevent it, and the harm materializes.[56] This means that States must strive to prevent State or non-State actors, including cybercriminals, from conducting cyber operations against the rights of other States.

28. Costa Rica believes that this obligation applies online as it does offline. It covers acts that contravene the sovereign rights of another State, such as ransomware[57] and cyber electoral interference,[58] whether or not these are perpetrated by a State or a non-State actor. Though this does not entail a general monitoring obligation, States must exercise a reasonable degree of vigilance over their networks. They must also put in place certain basic protective measures in line with their capabilities and other obligations under international law. Examples of diligent behavior in the cyber context may include the enactment of cybercrime legislation, the notification of cyber incidents to the victim State, and the establishment of a Computer Emergency Response Team and National Points of Contact.[59]

---

[51] International Law Association (ILA), *Study Group on Due Diligence, 2nd Report* (2016), at 2.
[52] Ibid, at 2-4.
[53] Ibid.
[54] *Corfu Channel Case* (*United Kingdom v Albania*), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.
[55] *Island of Palmas case* (n 32), at 839.
[56] Article 14(3), ILC Articles (n 8).
[57] The Oxford Process, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations', ELAC, 4 October 2021, para. 4.
[58] The Oxford Process, 'The Oxford Statement on International Law Protections Against Foreign Electoral Interference Through Digital Means', ELAC, 28 October 2020.
[59] GGE 2021 Report (n 1), paras 27, 65-66, 68, 76.

29. In Costa Rica's view, States also have **a general obligation to 'take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof'**, where such harm originates from their territory or jurisdiction and significantly affects persons, property, or the environment in other States.[60] This customary obligation applies to the physical consequences of significant transboundary harms beyond the ecological environment, whether or not the activity causing the harm is lawful or not under international law.[61] Costa Rica also believes that this duty applies to non-physical harms to persons, property or the environment, including those caused through or to ICTs.[62] Examples include instances of online incitement to violence, hostility or discrimination and disinformation campaigns causing harm to individuals, irrespective of whether they are contrary to a State's sovereign or other rights.

30. A standard of due diligence is also found in certain obligations under international human rights law and international humanitarian law, addressed below.

International human rights law

31. As affirmed by the UN Human Rights Council, human rights apply online just as they do offline.[63] States have obligations to respect, protect and ensure the enjoyment of a range of human rights, including civil and political rights as well as social, economic and cultural rights.[64]

32. Under certain human rights treaties, such as the International Covenant on Civil and Political Rights[65] and the American Convention on Human Rights,[66] those obligations are subject to a State's jurisdiction. In Costa Rica's view, jurisdiction goes beyond a State's territory, areas or persons under its physical control. It extends to all human rights over whose enjoyment the State exercises power or effective control, regardless of any physical proximity.[67] This means that, under those treaties, States must respect, protect and ensure human rights that are exercised online or via ICTs and over whose enjoyment a State exercises effective control.

---

[60] ILC, 'Draft articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries', A/56/10, Articles 1-3 and commentary; *Trail Smelter Case* (USA v Canada) (1941) 3 RIAA 1911, at 1963; *Pulp Mills on the River Uruguay, Case Concerning (Argentina v Uruguay)*, Judgment, 20 April 2010, ICJ Reports (2010) 14, paras 101, 187, 197, 204, 223.

[61] Fourth report on international liability for injurious consequences arising out of acts not prohibited by international law, by Mr. Robert Q. Quentin-Baxter, Special Rapporteur, A/CN.4/373 and Corr.1&.2, 1983, para. 17.

[62] E.g., Articles 1-5, 1936 International Convention concerning the Use of Broadcasting in the Cause of Peace.

[63] UN Human Rights Council, Res. 32/13 ('The promotion, protection and enjoyment of human rights on the Internet'), A/HRC/RES/32/13, 1 July 2016, para. 1.

[64] E.g., Article 2(1) International Covenant on Civil and Political Rights 1966, 999 UNTS 171 ('ICCPR'); Article 2(1), International Covenant on Economic, Social and Cultural Rights 1966, 993 UNTS 3 ('ICESCR').

[65] Article 2(1), ICCPR (n 64).

[66] Article 1(1), American Convention on Human Rights 1978, OAS Treaty Series No 36, 1144 UNTS 123.

[67] UN Human Rights Committee, HRC, General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, CCPR/C/GC/36, 30 October 2018, para. 63.

33. Human rights of particular importance in the online environment include the freedoms of opinion, expression, information, and assembly, as well as the rights to privacy and non-discrimination. Women have been particularly affected by cybercrime and other malicious cyber operations, including electronic surveillance, hate speech, doxing, cyber bullying, and harassment. Thus, Costa Rica reminds States of their obligations to respect, protect and ensure the rights of women online, including those laid down in the Convention on the Elimination of All Forms of Discrimination against Women.[68] Furthermore, the COVID-19 pandemic highlighted how cyber operations may also affect the rights to life and health.

34. Most human rights are not absolute and thus subject to limitation in certain circumstances. In this regard, Costa Rica notes that measures to protect the rights of States and individuals in cyberspace may often clash with certain individual human rights and must be balanced against them. For instance, to tackle online disinformation, the rights to receive and impart information freely on the Internet may be limited. Costa Rica stresses that the test for assessing the lawfulness of such limitations generally requires States to assess whether the limitation is grounded in sufficiently clear and accessible laws (legality), fulfils a legitimate purpose (legitimacy), and is necessary and proportionate to achieve this aim (necessity and proportionality).[69] This test must always be applied when the application of the rights and obligations discussed above implicates human rights online.

Use of force

35. Under Article 2(4) of the UN Charter and its customary counterpart, States 'shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state'. In Costa Rica's view, a State uses force against another State if it causes damage to persons or property in the territory of another State. This is true whether or not the military or other armed forces are involved, and regardless of the level of intensity of any hostilities between the States involved.

36. As noted earlier, **the prohibition on the use of force applies irrespective of the type of weapon employed by a State.**[70] Thus, **a cyber operation may amount to a prohibited use of force if it can cause harm or destruction analogous to a conventional weapon**.[71] In Costa Rica's view, this assessment is to be carried out on the basis of a comparison between the **effects** of a cyber operation and those of an operation carried out by conventional weapons that would constitute a prohibited use of force.[72] Although this assessment can only be carried out on a case-by-case basis, examples of cyber operations likely amounting to a prohibited use of force include those causing physical harm to individuals or significant

[68] UN General Assembly, Convention on the Elimination of All Forms of Discrimination Against Women (1981) 1249 UNTS 13.
[69] E.g., UN Human Rights Council, 'The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights', A/HRC/48/31, 13 September 2021, para. 8; UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression', A/67/357, 7 September 2012, para. 41.
[70] *Nuclear Weapons case* (n 6), para. 39.
[71] *Tallinn Manual 2.0* (n 4), Rule 69, paras 8-9, at 333.
[72] Ibid, Rule 69, para. 1, at 330.

destruction of property, as well as those permanently disabling operating systems controlling critical infrastructure, such as an electrical grid or a water and sanitation station.

37. **A prohibited threat or use of force must be distinguished from an armed attack**. In accordance with Article 51 of the UN Charter and customary international law, an armed attack triggers the right of **States to exercise individual or collective self-defense**.[73] In Costa Rica's view, to give rise to the right of self-defense, an armed attack must be attributable to a State, in cyberspace as in any other context.[74] As noted by the ICJ, armed attacks are the 'most grave' forms of use of force.[75] For Costa Rica, this assessment is to be carried out on the basis of a comparison between the **scale and effects** of a cyber operation and those of an operation by conventional weapons that would constitute an armed attack.[76] Examples of cyber operations potentially constituting armed attacks are those causing significant loss of life and destruction of critical infrastructure.[77]

International humanitarian law

Applicability of international humanitarian law

38. Costa Rica joins the global consensus of States that **international humanitarian law (IHL) is applicable in cyberspace and to cyber operations during armed conflicts**. As noted earlier, the International Court of Justice observed that IHL applies to 'all forms of warfare and to all kinds of weapons'.[78] In Costa Rica's perspective, there is no doubt that this extends to all uses of ICTs in situations of and connected to armed conflicts.

39. Costa Rica is also of the view that **affirming the application of IHL to the use of ICTs during armed conflict does not legitimize cyber warfare or encourage the militarization of cyberspace in any way**. IHL is a body of law that is restrictive in nature, and therefore it acts as a constraint, not an enabler of conflict. In addition, IHL imposes important limits on the militarization of cyberspace by prohibiting the development of new weapons or other military cyber capabilities that would be inconsistent with IHL, as detailed later in this position (see para. 56).

Cyber operations and armed conflicts

40. **IHL applies only in situations of armed conflict**.[79] During peacetime, certain additional measures must be taken to ensure respect for IHL in the event an armed conflict occurs. Those relevant in the ICT context include the duties to disseminate and train IHL, to adopt

[73] *Nicaragua case* (n 11), para. 191; *Tallinn Manual 2.0* (n 4), Rule 71, para. 6, at 341.
[74] *Armed Activities on the Territory of the Congo, Congo, the Democratic Republic of the v Uganda*, Judgment, Merits, [2005] ICJ Rep 168, paras 146-147; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, [2004] ICJ Rep 136, para. 139.
[75] *Nicaragua case* (n 11), para. 191.
[76] Ibid, para. 195; *Tallinn Manual 2.0* (n 4), Rule 71, paras 6-7, at 341.
[77] Ibid, para. 8, at 341.
[78] *Nuclear Weapons case* (n 6), para. 86.
[79] GGE 2021 Report (n 1), para. 71(f).

certain implementing domestic legislation, to carry out legal reviews of new weapons, means and methods of warfare, or to take measures to protect civilians against the effects of attacks.[80]

41. The relationship between cyber operations and armed conflict can be one of two kinds. First, **cyber operations may occur as part of an ongoing armed conflict**. If such operations have a sufficient nexus with the conflict (e.g., they are conducted in conjunction with or in support of traditional kinetic military operations during an existing conflict), they are governed by IHL.

42. Second, resorting to **cyber operations may bring an armed conflict into existence**. In this regard, IHL distinguishes between two types of armed conflict: international armed conflict, and non-international armed conflict. An **international armed conflict** comes to existence 'whenever there is a resort to armed force between States'.[81] In Costa Rica's view, this includes the use of cyber operations by one State against another State, as long as those operations have effects comparable to classic kinetic operations.[82] For example, a cyber operation by one State designed or expected to cause an industrial facility located in another State to catch fire, resulting in human and material loss, could bring into existence an international armed conflict as defined under Article 2 common to the Geneva Conventions and such cyber operation would be subject to IHL.

43. A **non-international armed conflict** exists if there is 'protracted armed violence between governmental authorities and organized armed groups or between such groups within a State'.[83] In theory, such conflicts may be initiated by the use of cyber operations between these actors.[84] However, in practice, the required threshold of intensity is unlikely to be reached by cyber operations alone. For example, a single cyber operation by a non-State group that disrupts, or damages critical infrastructure would normally not amount in and of itself to a non-international armed conflict and would therefore not be governed by IHL.

Established international legal principles of IHL

44. Costa Rica agrees with the global consensus on the significance and applicability of the established international legal principles of IHL, which include the principles of humanity, necessity, distinction, and proportionality.[85]

45. The **principles of humanity and military necessity** underlie and inform the entire normative framework of IHL. All rules of IHL reflect a careful balance between these two principles, which in turn inform the interpretation of these rules. The two principles also impose limits beyond

[80] ICRC, 'When does international humanitarian law apply to the use of information and communications technologies?' (March 2023), fn. 12.
[81] ICTY, *Tadić* Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 70.
[82] ICRC, *Commentary on the Third Geneva Convention*, 2020, commentary on common Article 2, para. 288.
[83] ICTY, *Tadić* Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, para. 70.
[84] *Tallinn Manual 2.0* (n 4), Rule 83, para. 2, at 385–386.
[85] GGE 2015 Report (n 1), para. 28(d); GGE 2021 Report (n 1), para. 71(f); OEWG 2022 Annual Progress Report (n 1), para. 15(b)(ii).

specific rules, including in the ICT environment.[86] In Costa Rica's view, this means that even if a cyber operation during an armed conflict is not specifically prohibited by a rule of IHL, to be lawful it must nonetheless comply with the principles of military necessity and humanity.

46. The **principle of distinction** requires that parties to an armed conflict distinguish at all times between civilians and combatants and between civilian objects and military objectives, including in the ICT environment. Cyber operations may only be directed against combatants or military objectives. Cyber operations must not be directed against civilians or civilian objects.[87] With respect to cyber infrastructure, the assessment of whether an object qualifies as a military objective must be done at the lowest level practically possible, i.e, at the level of each particular computer, cable, router, or other specific device that can be separated from a network or a system as a whole.

47. The **principle of proportionality** prohibits parties to armed conflicts from launching a cyber-attack against a military objective, which may be expected to cause incidental civilian harm that would be excessive in relation to the concrete and direct military advantage anticipated.[88] In Costa Rica's view, the incidental harm to be taken into consideration includes any incidental loss of functionality of civilian computers, systems or networks. For Costa Rica's understanding of the notion of loss of functionality, refer to para. 20 of this position.

Prohibition of attacks against civilian objects

48. Under IHL, **direct attacks against civilian objects are prohibited**.[89] In Costa Rica's view, this prohibition also governs the use of cyber means and methods of warfare.

49. Costa Rica defines a **cyber-attack** under IHL as any conduct initiated in or through cyberspace that is designed or can be reasonably expected to cause injury or death to persons or damage or destruction to objects. For these purposes, Costa Rica understands damage to include the disabling – temporary or permanent, reversible or not – of the targeted computer, system, or network. For the avoidance of doubt, this means that the existence of physical damage to objects or injury or death to persons is not required for an operation to constitute an attack under IHL. Conversely, mere network intrusion and exfiltration of data falls below the threshold of attack under IHL. In Costa Rica's perspective, encrypting data through ransomware, despite being temporary and reversible, would be considered an attack under IHL and therefore must not be directed against civilian systems.

50. Costa Rica endorses the view that **civilian data constitute civilian objects** under IHL and must be protected accordingly. Civilian datasets, including medical data, social security data, tax records, corporate and financial data, or electoral lists, are critical components of digitalized societies and play a vital role in the functioning of many aspects of civilian life. Deleting or damaging such data can have severe consequences for government services and private businesses, potentially causing more harm to civilians than the destruction of physical

[86] ICRC, 'The Principles of Humanity and Necessity' (March 2023).
[87] ICRC, 'The Principle of Distinction' (March 2023).
[88] ICRC, 'The Principle of Proportionality' (March 2023).
[89] Additional Protocol I, Article 52; ICRC, Customary International Humanitarian Law Study, Rule 7.

objects. Before the digital revolution, such data was stored in the form of paper files that were protected under IHL. Therefore, in Costa Rica's view, the protection of civilian objects under IHL extends to civilian data.

Prohibition of indiscriminate attacks

51. Under IHL, **indiscriminate attacks**, i.e., those of a nature to strike military objectives and civilians or civilian objects without distinction, are prohibited, including when carried out by cyber operations.[90] For example, releasing a computer virus that is designed to spread and cause harmful effects uncontrollably constitutes a prohibited indiscriminate attack, because such capability would be unable to distinguish between military and civilian systems as is required under IHL.

Precautions

52. States must put in place effective measures to prevent or mitigate the risk of civilian harm posed by the use of military cyber capabilities ("**active precautions**"). In the conduct of cyber operations, IHL requires that parties to an armed conflict take constant care to spare the civilian population, individual civilians, and civilian objects.[91] To avoid unintended consequences, cyber operators must have a thorough understanding of the degree to which the target networks and systems are interconnected and of the risks of unintended spread of malware or other cyber operations, including any indirect effects. In Costa Rica's view, this must include a consideration of the differentiated impacts that cyber operations may have on women, girls, members of the LGBTQ+ community and other vulnerable groups. At every stage, States must involve expertise from a wide range of sources and ensure that this is put into straightforward language for the relevant decision makers.

53. In relation to those cyber operations that qualify as attacks, parties to an armed conflict must, among other measures, take all feasible precautions to verify that the objectives to be attacked qualify as military objectives, as well as to avoid or at least minimize incidental civilian harm, including harm caused by indirect or reverberating effects, from such attacks.[92] A variety of technical measures can be considered, such as system-fencing, geo-fencing, or kill switches. Furthermore, if a party to an armed conflict determines that a planned cyber operation would shut down enemy command systems, but also incidentally disrupt civilian public services like water supply, it must suspend the attack until it can satisfy itself that the attack would be consistent with the applicable rules of IHL, including the prohibition of disproportionate attacks.

---

[90] Additional Protocol I, Article 51(4); ICRC, Customary International Humanitarian Law Study, Rules 11-12. Indiscriminate attacks are those: (a) which are not directed at a specific military objective; (b) which employ a method or means of combat which cannot be directed at a specific military objective; or (c) which employ a method or means of combat the effects of which cannot be limited as required by international humanitarian law; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

[91] Additional Protocol I, Article 57(1); ICRC, Customary International Humanitarian Law Study, Rule 15.

[92] Additional Protocol I, Article 57(2) and (3); ICRC, Customary International Humanitarian Law Study, Rules 15–21.

54. States must put in place effective measures to protect the civilian population against the dangers resulting from military cyber operations ("**passive precautions**"). Parties to an armed conflict that may be targeted by cyber operations have a responsibility to minimize the danger of civilian harm caused by such operations.[93] Some of these measures may need to be implemented already in peacetime. For instance, States should cultivate a strong culture of cyber resilience throughout their societies and ensure that their critical infrastructure and other infrastructure used by civilians is protected to the highest possible standard. States should also have an adequate understanding of the critical dependencies in their networks in order to be able to restore their functionality in the event of a destructive or disruptive attack. Moreover, whenever feasible, armed forces should segregate military networks from civilian cyber infrastructure, thus limiting the spread of harmful effects onto civilian networks in case a military network is attacked. Similarly, civilian systems should be designed so as to avoid dependence on systems that may qualify as military objectives, thus reducing the risk of civilian harm. States should assist each other with capacity building to ensure that all States have the means to protect themselves against harmful cyber operations. Finally, during armed conflict, States should avoid involving civilians in military cyber operations as doing so may expose them to a grave risk of harm.

Choice of means and methods of warfare

55. **The right of the parties to an armed conflict to choose means and methods of warfare, including cyber capabilities, is not unlimited.**[94] In particular, parties to an armed conflict are barred from using means and methods of warfare that are expressly prohibited by IHL. For instance, the use of poison or poisoned weapons is prohibited.[95] This means that a cyber operation that is designed or expected to result in poisoning the water supply is specifically prohibited by IHL. This is true irrespective of whether the operation would amount to an attack or if the water supply would qualify as an object indispensable to the civilian population (on which see paras 49 and 61, respectively). Similarly, a cyber operation directed at a factory or other infrastructure containing or using toxic chemicals, designed or expected to cause harm through their release, is prohibited.[96]

Legal review of new cyber capabilities

56. **The legality of all new weapons, means and methods of warfare, including cyber capabilities, must be systematically assessed by all States**. IHL requires that in the study, development, acquisition or adoption of any new weapon, means or method of warfare, States must determine whether its employment would, in some or all circumstances, be prohibited

[93] Additional Protocol I, Article 58; ICRC, Customary International Humanitarian Law Study, Rules 22-24.
[94] Additional Protocol I, Article 35(1).
[95] Hague Regulations (1907), Article 23(a); ICRC, Customary International Humanitarian Law Study, Rule 72.
[96] Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (1993), Article 1; ICRC, Customary International Humanitarian Law Study, Rule 74.

under IHL or any other applicable rule of international law.[97] Costa Rica considers this obligation to reflect customary international law binding on all States. In Costa Rica's view, the obligation is also applicable to cyber means and methods of warfare. For instance, this would include an obligation to review whether ransomware or other forms of malware designed or expected to be employed in times of armed conflict are capable of being used in accordance with IHL.

Information and psychological operations

57. IHL sets important **limits on information and psychological operations during armed conflicts, including when conducted through digital communication platforms**. In particular, parties to armed conflicts must 'not encourage persons or groups engaged in the conflict to act in violation' of IHL.[98] Moreover, IHL prohibits parties to armed conflicts from threatening that no quarter will be given to surrendering enemy soldiers,[99] from spreading fear and terror among civilian populations,[100] or from using propaganda to secure voluntary enlistment of protected persons in occupied territories.[101] In Costa Rica's vision, these prohibitions apply offline as well as online, and irrespective of which means of communication are used. The use of information or psychological operations must also not amount to outrages against the dignity of either civilians or captured soldiers, for instance by exposing protected civilians or prisoners of war to public curiosity through disclosing their photographs or videos on social media.[102] Overall, parties to an armed conflict should integrate a gender perspective in the planning and execution of information and psychological operations. This might include tailoring messaging campaigns to address the specific circumstances and needs of women, girls, members of the LGBTQ+ community and other vulnerable groups in conflict-affected areas.

Specific protection

58. IHL affords **specific protection to certain persons, objects and activities**, such as medical personnel and units; humanitarian personnel and relief objects; and objects indispensable to the survival of the civilian population.

59. Under IHL, **medical facilities** must be respected and protected by the parties to the conflict at all times.[103] The obligation to respect and protect such facilities entails that it is also

[97] Additional Protocol I, Article 36.
[98] ICJ, *Military and Paramilitary Activities in and against Nicaragua case*, Judgment, 1986, para. 220; see also Oxford Process, 'The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities' (June 2021), para. 8.
[99] Additional Protocol I, Article 40; ICRC, Customary International Humanitarian Law Study, Rule 46.
[100] Additional Protocol I, Article 51(2); ICRC, Customary International Humanitarian Law Study, Rule 2.
[101] Geneva Convention IV, Article 51.
[102] Geneva Convention III, Article 13(2); Geneva Convention IV, Article 27(4); see also ICRC, *Commentary on the Third Geneva Convention*, 2020, commentary on Article 13, para. 1624.
[103] Geneva Convention I, Article 19; Geneva Convention II, Article 12; Geneva Convention IV, Article 18; Additional Protocol I, Article 12; Additional Protocol II, Article 11; ICRC, Customary International Humanitarian Law Study, Rules 25, 28, and 29.

prohibited to interfere with their functioning using cyber means, irrespective of whether doing so would amount to an attack as understood under IHL. In Costa Rica's view, this obligation also encompasses a prohibition against deleting or tampering with medical data (a category that includes data necessary for the proper use of medical equipment, tracking medical supplies, and personal medical data required for patient treatment).

60. Under IHL, **personnel and objects engaged in or used for humanitarian relief operations** must be respected and protected by the parties to the conflict at all times.[104] In Costa Rica's view, this obligation entails a prohibition against attacking or otherwise harming humanitarian relief personnel and objects, an obligation to take feasible measures to protect them against harm, and a prohibition against using cyber operations to interfere with the impartial efforts to provide humanitarian relief, even if this interference would not rise to the level of attack. Costa Rica understands the obligation to respect and protect relief personnel and objects as also covering the associated data.

61. Under IHL, it is prohibited to attack, destroy, remove or render useless **objects indispensable to the survival of the population**, including when using cyber operations.[105] The protection under this rule extends to the ICT equipment and the data needed to operate such objects. Thus, for example, a cyber operation against food production systems, drinking water installations, or wastewater management systems would be a violation of IHL even if it did not reach the threshold of attack under IHL.[106]

Duty to respect and ensure respect for IHL

62. All States and parties to armed conflicts have an overarching obligation to respect and ensure respect for IHL in all circumstances, including with regard to cyber operations during armed conflicts.[107] As noted in para. 40, this general duty entails that certain additional measures with relevance to the use of ICTs must be taken already in peacetime to ensure respect for IHL in the event an armed conflict occurs. In addition, States must investigate and prosecute persons suspected of having committed war crimes, including through the use of ICTs during armed conflict.[108] States must also refrain from transferring cyber weapons, means and methods of warfare where there is a clear risk that these would be used to commit IHL violations.

Neutrality

63. The **law of neutrality is applicable to cyber operations carried out during an international armed conflict**, and it protects the populations and the cyber infrastructure in

[104] Geneva Convention IV, Articles 59, 70(4), and 71(2); ICRC Customary International Humanitarian Law Study, Rules 31–32.
[105] Additional Protocol I, Article 54; ICRC, Customary International Humanitarian Law Study, Rule 54.
[106] *Tallinn Manual 2.0* (n 4), Rule 141, para. 6, at 533.
[107] Geneva Conventions, common Article 1; Additional Protocol I, Article 1; ICRC, Customary International Humanitarian Law Study, Rules 139 and 144.
[108] Geneva Conventions I–IV, Articles 49/50/129/146; Additional Protocol I, Article 85; ICRC, Customary International Humanitarian Law Study, Rule 158.

neutral States from the effects of such conflicts.[109] Costa Rica understands the term "**neutral State**" as referring to any State which is not a party to an ongoing international armed conflict.

64. **Parties to an international armed conflict** are prohibited from carrying out cyber operations against and from cyber infrastructure located in the territory, and under the exclusive control of, neutral States.[110] In Costa Rica's perspective, they must also refrain from engaging in cyber operations that are reasonably expected to cause incidental harm to cyber infrastructure situated on the territory of neutral States.

65. Under the law of neutrality, a **neutral State** must not knowingly allow any use of cyber infrastructure located in its territory, or under its exclusive control, by parties to an international armed conflict for hostile purposes. This obligation is one of due diligence and is thus subject to the means reasonably available to the neutral State in question as well as its knowledge – actual or constructive – of such hostile uses of its cyber infrastructure. Conversely, the neutral State is not obliged to prevent parties to the conflict from using its networks solely for communication purposes.

[109] See ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996, para. 89.
[110] Hague Convention V, Articles 1–3; Hague Convention XIII, Articles 1, 2, and 5; *Tallinn Manual 2.0* (n 4), Rules 150–151.