International Law applicable in cyberspace

international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx

Table of contents

Introduction

1. The recent rise in malicious online activities and rapid developments in cyber capabilities have led States to consider questions on how international law applies to State activity in cyberspace.
2. Canada supports the rules-based international order (RBIO), grounded in respect for international law. Canada considers that the RBIO extends to moderating State behaviour in cyberspace.[Footnote 1] To this end, Canada has been active in multilateral efforts to create the framework for responsible State behaviour in cyberspace.[Footnote 2]
3. Canada supports calls for States to develop and publish their national views on ***how*** international law applies in cyberspace. States have started stepping forward to issue statements on their national views. Canada is now in a position to do this ourselves. This follows several years of intensive consultations, reflection on the views of a range of States, and participation in formal and informal processes with States and other key stakeholders.[Footnote 5]
4. Canada believes that the articulation of national positions on ***how*** international law applies to State action in cyberspace will increase international dialogue and the development of common understandings and consensus on lawful and acceptable State behaviour.[Footnote 6] These statements can help reduce the risk of misunderstandings and escalation between States arising from cyber activities.
5. Canada continues to strongly advocate for capacity-building on the application of international law in cyberspace. We are committed to ensuring that the broadest possible group of States participates effectively in addressing these important questions, which increasingly affect all States.
6. This statement sets out Canada's current view on key aspects of international law applicable in cyberspace and explains how these apply. Where possible we have included examples to better illustrate our position on a given aspect. Cyber-related challenges are magnified by rapid technological developments and the ever-increasing activities of malicious actors. Recognizing the ongoing nature of technological change, Canada will continue to develop and publicise its views, including through dialogue with other States and stakeholders.

General application of international law

8. Canada affirms that international law applies to the activities of every State in cyberspace. This includes the United Nations Charter (UN Charter) in its entirety and customary international law.[Footnote 7] Canada recognizes the obligations of every State flowing from the principle of sovereignty to: refrain from the threat or use of force; settle disputes peacefully; and refrain from intervention in the internal affairs of other States. Canada further recognizes the obligations arising, in a non-exhaustive manner, from international human rights law (IHRL), international humanitarian law (IHL) and in relation to the law of State responsibility.
9. Canada supports agreed voluntary, non-binding norms for responsible State behaviour in cyberspace,[Footnote 8] as a complement to international law, and continues to promote their implementation by all States.[Footnote 9] Such voluntary norms do not replace or alter States' binding obligations or rights under international law: they provide additional specific guidance on what constitutes responsible State behaviour.[Footnote 10]

Sovereignty

10. Sovereignty is a fundamental element of international law and international relations. It is axiomatic that the principle of sovereignty applies in cyberspace, just as it does elsewhere. It animates a number of obligations for all States.
11. In the relations between States, sovereignty signifies independence. It confers to each State the exclusive right to exercise the functions of a State within its territory.[Footnote 11]
12. This concept is also reflected in Canadian jurisprudence where Canada's highest court found that "sovereignty" referred to "the various powers, rights and duties that accompany statehood under international law…"[Footnote 12] and "…one of the organizing principles of the relationships between independent states".[Footnote 13]
13. Territorial sovereignty is a rule under international law.[Footnote 14] Every State must respect the territorial sovereignty of every other State. States enjoy sovereignty over their territory, including in particular infrastructure located within their territory and activities associated with that infrastructure. An infringement upon the affected State's territorial integrity, or an interference with or usurpation of inherently governmental functions of the affected State, would be a violation of territorial sovereignty.[Footnote 15]
14. In assessing the possible infringement of a State's territorial sovereignty, several key factors must be considered. The scope, scale, impact or severity of disruption caused, including the disruption of economic and societal activities, essential services, inherently governmental functions, public order or public safety must be assessed to determine whether a violation of the territorial sovereignty of the affected State has taken place.

15. In general, the impact or severity of cyber effects will be evaluated in the same manner and according to the same criteria as for physical activities. Cyber activities that rise above a level of negligible or *de minimis* effects, causing significant harmful effects within the territory of another State without that State's consent, could amount to a violation of the rule of territorial sovereignty with respect to the affected State. It is also important to note that cyber activities with effects in another State do not constitute physical presence in the territory of that State. As such, territorial sovereignty is not violated by virtue merely of remote activities having been carried out on or through the cyber infrastructure located within the territory of another State. Furthermore, cyber activities carried out remotely from within Canada with negligible effects in a foreign State do not involve an extraterritorial exercise of enforcement jurisdiction by Canada.
16. Cyber activities that cause a loss of functionality with respect to cyber infrastructure located within the territory of the affected State may also constitute a violation of territorial sovereignty if the resulting loss of functionality causes significant harmful effects similar to those caused by physical damage to persons or property. For example, a violation of the territorial sovereignty will occur when the cyber activity creates a significant harmful effect that necessitates the repair or replacement of physical components of cyber infrastructure in the affected State. The loss of functionality of physical equipment that relies on the affected infrastructure in order to operate could also form part of the violation. The assessment of the effects includes both intended and unintended consequences that reach the threshold required to trigger a violation.
17. The rule of territorial sovereignty does not require consent for every cyber activity that has effects, including some loss of functionality, in another State. Activities causing negligible or *de minimis* effects would not constitute a violation of territorial sovereignty regardless of whether they are conducted in the cyber or non-cyber context. Nor are States precluded by the rule of territorial sovereignty from taking measures that have negligible or *de minimis* effects to defend against the harmful activity of malicious cyber actors or to protect their national security interests. For example, Canada considers that a cyber activity that requires rebooting or the reinstallation of an operating system is likely not a violation of territorial sovereignty.
18. The other key basis for assessing a violation of territorial sovereignty is whether a cyber activity interferes with or usurps the inherently governmental functions of another State. Cyber activities that have significant harmful effects on the exercise of inherently governmental functions would constitute an internationally wrongful act. For Canada, this would include government activities in areas such as health care services, law enforcement, administration of elections, tax collection, national defence and the conduct of international relations, and the services on which these depend. There can be a violation of territorial sovereignty by way of effects on governmental functions regardless of whether there is physical damage, injury, or loss of functionality. An example would be a cyber activity that interrupts health care delivery by blocking access to patient health records or emergency room services, resulting in risk to the health or life of patients.

19. Importantly, some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law.[Footnote 16] They may however be prohibited under the national laws of a State.[Footnote 17]
20. It is possible that a series of cyber activities could lead to significant harmful effects that violate the rule of territorial sovereignty. This is the case even if the individual cyber activity on its own would not reach this threshold.
21. Canada will assess whether a violation of territorial sovereignty has occurred on a case-by-case basis. As noted below, Canada believes further State practice and *opinio juris* will help clarify the scope of customary law in this area over time. In any event, Canada considers that the existence of varied approaches to assessing the legality of cyber activities should not prevent States from agreeing that particular malicious cyber activities are internationally wrongful acts.

Non-Intervention

22. State cyber activities may breach the foundational international law prohibition of intervention in the internal or external affairs of another State. This would be the case where both of the following conditions are met:
    - the activities aim to interfere with the internal or external affairs of the affected State involving its inherently sovereign functions, known as *domaine réservé*[Footnote 18]; and
    - the activities would cause coercive effects that deprive, compel, or impose an outcome on the affected State on matters in which it has free choice.[Footnote 19]
23. In its most serious form, coercion may arise through the threat or use of force but could also arise where a cyber activity is designed to deprive the affected State of its freedom of choice. Coercion must be distinguished from other conduct such as public diplomacy, criticism, persuasion, and propaganda.
24. An example of a prohibited intervention would be a malicious cyber activity that hacks and disables a State's election commission days before an election, preventing a significant number of citizens from voting, and ultimately influencing the election outcome. Another example would be a malicious cyber activity that disrupts the functioning of a major gas pipeline, compelling the affected State to change its position in bilateral negotiations surrounding an international energy accord.
25. Whether or not a cyber activity meets the threshold for a violation of the rule on territorial sovereignty or rises to the level of a violation of the rule against intervention will be determined on a case-by-case basis. As with the thresholds for violations of territorial sovereignty, Canada believes that further State practice and *opinio juris* will help clarify the thresholds for the rule of non-intervention, and the scope of customary law in this area over time.

Due Diligence

26. No State should knowingly allow its territory to be used for acts contrary to the rights of other States.[Footnote 20] This also applies in cyberspace. A State that has knowledge of a malicious cyber activity is expected to take all appropriate and reasonably available and feasible steps to stop ongoing or temporally imminent cyber activities that result or would result in significant harmful effects that impact the legal rights of another State.
27. The precise threshold that triggers this expectation will depend on the totality of the circumstances in that situation. This would include whether the State has knowledge of the wrongful acts, its technical and other capacities to detect and stop these acts, and what is reasonable in that case. For example, a State with limited technical capabilities would not likely be expected to respond if it failed to detect a malicious cyber activity emanating from or through cyber infrastructure on its territory. However, once aware, the State would be expected to respond.

State Responsibility

28. The international law of State responsibility applies across the whole spectrum of substantive areas of international law, including in cyberspace. It governs such issues as the attribution of internationally wrongful acts to States. It also addresses circumstances precluding wrongfulness, including countermeasures, and possible remedies. The law of State responsibility is not concerned with the legality of the use of force, including in self-defence, which is a separate area of international law.
29. In Canada's view, this well-established body of international law is not only applicable, but highly relevant in relation to contemporary cyber activities. To date, all publicly known malicious cyber activities have been widely interpreted by States as falling below the threshold (or thresholds) of the threat or use of force or armed attacks.

Internationally Wrongful Acts

30. An internationally wrongful act in the cyber context is a cyber-related action or omission that:
    - constitutes a breach of an international legal obligation, whether to another State or the entire international community; and
    - is attributable to a State under international law.
31. International law recognises exceptions to what would otherwise be internationally wrongful acts. Examples include cases of self-defence and countermeasures.

Attribution

32. Canada applies the customary international law on State responsibility to attribute wrongful conduct in cyberspace. Under the law of State responsibility, an important element is that of attribution, which involves the identification of a State as legally responsible for an internationally wrongful act. A State can be responsible directly, or indirectly where a non-State actor has acted on the instructions of, or under the direction or control of, that State.[Footnote 21] In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through non-state actors who act on a State's instruction or under its direction or control.[Footnote 22]
33. Attribution in its legal sense is of course distinct from the technical identification (or technical attribution) of the actor responsible for malicious cyber activity, whether State or non-State, as well as from the public denunciation of the responsible actor (political attribution). Further, Canada believes that the public attribution of internationally wrongful acts engages various political considerations beyond technical and legal attribution. To this end, States bear no obligation to publicly provide the basis upon which an attribution is made.

Countermeasures

34. Canada considers that States are entitled to use countermeasures in response to internationally wrongful acts including in cyberspace. The customary international law of State responsibility defines limits in the exercise of the right to take countermeasures, being actions that would otherwise be unlawful.[Footnote 23] Countermeasures may not be taken in retaliation, but only to induce compliance, and directed at the State responsible for the internationally wrongful act. They may not constitute the threat or use of force, must be consistent with other peremptory norms of international law, and they must be proportional.
35. Lawful countermeasures in response to internationally wrongful cyber acts can be non-cyber in nature, and can include cyber operations in response to non-cyber internationally wrongful acts.
36. A State taking countermeasures is not obliged to provide detailed information equivalent to the level of evidence required in a judicial process to justify its cyber countermeasures; however, the State should have reasonable grounds to believe that the State that is alleged to have committed the internationally wrongful act was responsible for it. The precise scope of certain procedural aspects of countermeasures, such as notification, needs to be further defined through State practice given the unique nature of cyberspace.[Footnote 24]
37. Assistance can be provided on request of an injured State, for example where the injured State does not possess all the technical or legal expertise to respond to internationally wrongful cyber acts. However, decisions as to possible responses remain solely with the injured State. Canada has considered the concept of "collective cyber countermeasures" but does not, to date, see sufficient State practice or *opinio juris* to conclude that these are permitted under international law. Canada distinguishes "collective cyber countermeasures" from actions taken in "collective self-defence" including measures taken in cyberspace.

International human rights law (IHRL)

38. It is beyond dispute that international human rights law applies to activities in cyberspace. For many years, Canada has consistently advanced that all individuals enjoy the same human rights, and States are bound by the same human rights obligations, online just as offline.[Footnote 25] States' activities in cyberspace must be in accordance with their international human rights obligations as expressed in the international human rights treaties to which they are a party, and in customary international law.
39. Canada notes that according to Article 2(1) of *The International Covenant on Civil and Political Rights,* each State Party is required to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in that instrument, without distinction.[Footnote 26]
40. The internationally recognized human rights that are of particular concern in relation to cyberspace include the right to freedom of expression and to hold opinions without unlawful interference, freedom of association and of peaceful assembly, freedom from discrimination, and the right not to be subjected to arbitrary or unlawful interference with one's privacy or correspondence.

Peaceful Settlement of disputes

41. A central, and at times overlooked, rule of international law is the obligation of every State, under the UN Charter, to seek the settlement of disputes by peaceful means.[Footnote 27] This is closely related to the prohibition of the threat or use of force.[Footnote 28] Like that prohibition, it applies in cyberspace just as it does elsewhere. Thus, Canada considers that in line with the UN Charter, in case of disputes States may seek solutions through negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.
42. The obligation to seek the settlement of disputes by peaceful means is not unlimited, nor does it diminish other international legal obligations or rights, such as the inherent right of self-defence.
43. Canada considers that a State may always respond to an unfriendly act or an internationally wrongful act with unfriendly acts provided they are not contrary to international law.

Threat or use of Force

44. Article 2(4) of the UN Charter requires that States refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the UN. This also applies in cyberspace. In general, cyber activities that amount to such a threat or use of force are unlawful, with recognised exceptions under international law.

45. In Canada's view, cyber activities may amount to such a threat or use of force where the scale and effects are comparable to those from other operations that constitute the use of force at international law. Canada will assess cyber activities that may amount to a threat or use of force on a case-by-case basis.

Self-Defence against Armed Attack

46. Canada considers that the inherent right of self-defence if an armed attack occurs against a State also applies in cyberspace.[Footnote 29]
47. Canada will respond to cyber activities that amount to an armed attack in a manner that is consistent with international law. Canada's response may include cyber operations. The right to self-defence is both an individual and collective right of States.

International Humanitarian Law (IHL)

48. IHL applies to cyber activities conducted in the context of both international and non-international armed conflict and regulates the conduct of hostilities and protects the victims of armed conflict.[Footnote 30] In any armed conflict, the right of parties to choose means and methods of warfare is not unlimited.
49. Cyber activities are an attack under IHL, whether in offence or defence, where their effects are reasonably expected to cause injury or death to persons or damage or destruction to objects.[Footnote 31] This could include harmful effects above a *de minimis* threshold on cyber infrastructure, or the systems that rely on it. Such cyber activities must respect relevant treaty and customary IHL rules applicable to attacks including those relating to distinction, proportionality, and the requirement to take precautions in attack.
50. States that are Parties to Additional Protocol I to the Geneva Conventions are required to review new weapons, means or methods of warfare to ensure compliance with IHL.[Footnote 32] This obligation applies in the context of cyber capabilities and activities, although not all cyber capabilities and activities will constitute a weapon or means or method of warfare.
51. Canada emphasises that acknowledging the application of IHL to cyber activities in armed conflict neither contributes to militarising cyberspace nor legitimises cyber activities that are unlawful.[Footnote 33]

Conclusion

52. With this statement, Canada joins the many other States which have publicised their views on how international law applies in cyberspace. We hope that States which have not yet done so will consider publishing their own statements as well and thus contribute to the emergence of common understandings.

53. To that end, Canada will continue to actively support capacity building on international law and cyberspace. Canada has found the process of consultations that led to this statement to be very beneficial in developing a deeper understanding of *how* international law applies to cyberspace.
54. Canada believes it is crucial for all States to move beyond discussions of general concepts and build common understandings of what constitutes unlawful conduct in cyberspace. Canada will continue to develop and publicise its positions, including through dialogue with other States and stakeholders, in its ongoing efforts to contribute to security and stability in cyberspace.

Footnotes

Footnote 1
Although cyberspace has no single agreed upon definition, it consists of interdependent networks of information technology structures—including the Internet, telecommunications networks, computer systems, embedded processors and controllers—as well as the software and data that reside within them: Canada Defence Terminology Standardization Board (DTSB) (2016).

Return to footnote 1 referrer

Footnote 2
This framework is based on the applicability of international law to State activities; voluntary, non-binding norms; and the development and implementation of practical confidence building measures to help reduce the risk of conflict stemming from cyber activities.

Return to footnote 2 referrer

Footnote 3
United Nations General Assembly (UNGA), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UNGAOR, 68th Sess, UN Doc A/68/98*(2013) (2013 GGE Report) (later adopted by the UNGA Resolution A/RES/68/243); UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGAOR, 70th Sess, UN Doc A/70/174 (2015) (2015 GGE Report) (later adopted by the UNGA Resolution A/RES/70/237); UNGA, *Report of the Open-ended working group on developments in the field of information and telecommunications in the context of international security,* UN Doc A/75/816 (2021) (2021 OEWG Report); UNGA, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 76th Sess,* UN Doc A/76/135 (2021) (2021 GGE Report) (both later adopted by UNGA Resolution A/RES/76/19).

Return to footnote 3 referrer

Footnote 4

Statements by Canada during the informal consultative meeting of the Group of Governmental Experts on Advancing Responsible State behaviour in Cyberspace in the context of international security (2019), online: www.un.org/disarmament/wp-content/uploads/2020/01/statements-canada-informal-consultative-meeting-gge-5-6-december.pdf.

Return to footnote 4 referrer

Footnote 5
2021 GGE Report, *supra* note 3; *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts,* at 73; The NATO Cooperative Cyber Defence Centre of Excellence, *International cyber law: interactive toolkit* (2022), online: https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

Return to footnote 5 referrer

Footnote 6
2021 OEWG Report, *supra* note 3 at 36-37, 39-40.

Return to footnote 6 referrer

Footnote 7
Charter of the United Nations (UN Charter), 26 June 1945 Can TS 1945 No.7.,online: <https://www.un.org/en/about-us/un-charter/full-text.

Return to footnote 7 referrer

Footnote 8
2015 GGE Report, *supra* note 3, which first established the eleven (11) non-binding, voluntary norms of responsible State behaviour; 2021 GGE Report, supra note 3; 2021 OEWG Report, supra note 3.

Return to footnote 8 referrer

Footnote 9
Chair's Summary, OEWG, 3rd substantive session, Annex, UN Doc A/AC.290/2021/CRP.3* (2021) 10-15.

Return to footnote 9 referrer

Footnote 10
2021 OEWG Report, *supra* note 3 at 25.

Return to footnote 10 referrer

Footnote 11

Island of Palmas (or Miangas) Case: United States v Netherlands, Award, (1928) 2 RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, Permanent Court of Arbitration [PCA], online*: <https://legal.un.org/riaa/cases/vol_II/829-871.pdf*.

Return to footnote 11 referrer

Footnote 12
R. v. Hape, 2007 SCC 26 (CanLII), [2007] 2 SCR 292, online: < https://canlii.ca/t/1rq5n.

Return to footnote 12 referrer

Footnote 13
Ibid at 43.

Return to footnote 13 referrer

Footnote 14
International law provides for exceptions to the rule on territorial sovereignty such as those actions (i) authorised by the United Nations Security Council; (ii) taken in self-defence in relation to an armed attack; (iii) consented to by the affected State; or (iv) that constitute countermeasures. These exceptions apply in cyberspace.

Return to footnote 14 referrer

Footnote 15
Schmitt, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2d ed (Cambridge: Cambridge University Press, 2017) at 20 para. 10 *[*hereinafter *Tallinn Manual 2.0]*.

Return to footnote 15 referrer

Footnote 16
Of note, espionage, while not *per se* wrongful under international law, could be carried out in a way that might violate international law. See generally *Tallinn Manual 2.0*, *supra* note 15, Rule 4 and its discussion of cyber espionage at 19 paras 7-9.

Return to footnote 16 referrer

Footnote 17
For example, in Canada economic espionage is a violation of section 19 of the *Security of Information Act* (R.S.C. 1985, c.O-5), and every person who commits an offence under subsection 19(1) is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years.

Return to footnote 17 referrer

Footnote 18

Inherently sovereign functions (also known as *domaine réservé*) include those matters in which a State may decide freely, such as political, economic, social, and cultural systems, as well as the formation of foreign policy.

Return to footnote 18 referrer

Footnote 19
Tallinn Manual 2.0 *supra* note 15, Rule 66 and accompanying commentary at 318 para 19, provides that "mere coercion does not suffice to establish a breach of the prohibition of intervention…[it] must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State."

Return to footnote 19 referrer

Footnote 20
See the discussion of the voluntary, non-binding UN GGE norms in the 2021 UN GGE Report, *supra* note 3 at 29-30, 42-46. Canada does not consider that the UN GGE consensus in 2015, and subsequently, on voluntary, non-binding norms touching on this matter precludes the recognition of a binding legal rule of due diligence under customary international law. Canada continues to study this matter.

Return to footnote 20 referrer

Footnote 21
A State may also engage international responsibility if it coerces another state or directs and controls it in the commission of an internationally wrongful act: International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts (Articles on State Responsibility), with commentaries, (2001)* Arts. 17, 18, online: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

Return to footnote 21 referrer

Footnote 22
Articles on State Responsibility, supra note 21,Art. 8.

Return to footnote 22 referrer

Footnote 23
Articles on State Responsibility, supra note 21, *A*rt. 22.

Return to footnote 23 referrer

Footnote 24
In this regard the law of state responsibility foresees cases where notification may not be required – *Articles on State Responsibility, supra* note 21,Art. 52(b).

Return to footnote 24 referrer

Footnote 25

Government of Canada, *Human rights and inclusion in online and digital contexts* (2022), online: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/internet_freedom-liberte_internet.aspx?lang=eng.

Return to footnote 25 referrer

Footnote 26
International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, 999 UNTS 171, online: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Return to footnote 26 referrer

Footnote 27
UN Charter, supra note 7, Art. 2(3), Art. 33(1); *Tallinn Manual 2.0, supra* note 15, Rule 65 at 303.

Return to footnote 27 referrer

Footnote 28
UN Charter, supra note 7, Art. 2(4).

Return to footnote 28 referrer

Footnote 29
UN Charter, supra note 7, Art. 51.

Return to footnote 29 referrer

Footnote 30
Tallinn Manual 2.0, supra note 15, Rule 80 at 375.

Return to footnote 30 referrer

Footnote 31
Tallinn Manual 2.0, supra note 15,Rule 92 at 415; see also generally Article 49(1) of *the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protections of Victims of International Armed Conflicts (Protocol I*), 8 June 1977, 1125 UNTS 3, online: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949.

Return to footnote 31 referrer

Footnote 32
Protocol I, supra note 31*,* Art. 36; see also generally *Tallinn Manual 2.*0 *supra* note 15*,* Rule 110 and accompanying commentary at 464.

Return to footnote 32 referrer

Footnote 33

The views of the International Committee of the Red Cross (ICRC) are a valuable reference on this point: ICRC, *Cyber operations during armed conflict are not happening in the a 'legal void' or 'grey zone'-they are subject to the established principles and rules of international humanitarian law*: Statement by the International Committee of the Red Cross to the UN Security Council Open Debate on Cyber Security, maintaining international peace and security in cyberspace (2021), online: https://www.icrc.org/en/document/cyber-operations-during-armed-conflict-are-not-happening-legal-void-or-grey-zone-they-are; ICRC, *The ICRC calls on all States to affirm that IHL applies to, and therefore restricts, cyber operations during armed conflicts:* Statement to the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, Informal Consultative meeting (2021), online: https://www.icrc.org/en/document/icrc-calls-all-states-affirm-ihl-applies-and-therefore-restricts-cyber-operations-during.

Return to footnote 33 referrer

Date Modified:

2022-04-22