An Roinn Gnóthaí Eachtracha
Department of Foreign Affairs

IRELAND

POSITION PAPER ON THE APPLICATION OF INTERNATIONAL LAW IN CYBERSPACE

Introduction

1. International law, including the Charter of the United Nations, applies in cyberspace. This has been acknowledged in two processes established by the United Nations General Assembly, namely the Group of Governmental Experts on advancing responsible state behaviour in cyberspace in the context of international security (GGE) as well as the Open-ended Working Group on security of and in the use of information and communications technologies (OEWG).

2. Ireland has published the present paper as a contribution to discussions at UN level, particularly in the context of its participation in the OEWG, aimed at developing a better shared understanding of how international law applies in cyberspace. It is hoped that these discussions will contribute to promoting responsible state behaviour in cyberspace and a more stable, secure, open, accessible and peaceful cyber environment with international law and the rules-based international order at its centre.

3. This paper does not by any means purport to offer an exhaustive or comprehensive analysis; rather it is aimed at providing a reasonably concise expression of Ireland's national position on some of the more relevant issues arising.

Principle of Sovereignty

4. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by states of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.[1] The principle of state sovereignty encompasses the concepts of territorial integrity and territorial authority, the independence of state powers, and the equality of states in the international order. A state enjoys a right to exercise jurisdiction in terms of regulation, adjudication and enforcement in relation to cyber infrastructure as well as persons engaging in cyber activities on its territory. A state may also be entitled, in limited circumstances, to exercise extraterritorial jurisdiction in accordance with international law.

5. The International Court of Justice (ICJ) in the *Nicaragua* case noted that "the principle of respect for state sovereignty […] is closely linked with the principles of prohibition of the

[1] A/70/174 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report (22 July 2015), [27].

use of force and non-intervention".[2] In line with the stated position of many other states, Ireland considers that respect for sovereignty is an obligation in its own right. A violation of state sovereignty by way of cyber activities is capable of amounting to an internationally wrongful act and triggering state responsibility, even if such a violation falls short of the threshold of non-intervention or the use of force.

6. A violation of a state's sovereignty may arise where a cyber-operation attributable to another state causes physical damage to ICT or other infrastructure (whether or not in state ownership or control), functional impairment to such infrastructure, interference with data, and/or secondary effects. The nature and consequences of a cyber-operation are relevant to determining whether a violation has occurred in any given case.

7. Sovereignty may not be relied on to justify a state's non-compliance with applicable obligations under international law. Ireland notes with regret that sovereignty has at times been relied on by some states as justification for cyber measures and/or restrictions within their jurisdiction – such as cyber surveillance or censorship – which compromise human rights, in particular the right to freedom of expression, freedom of thought, conscience and religion, and the right to privacy.

Principle of Non-Intervention

8. The principle of non-intervention in the internal affairs of states, a corollary of the principle of sovereignty, involves the right of every sovereign state to conduct its affairs without interference.[3] The principle of non-intervention, outside the context of use of force, applies to one state's actions in relation to another state where two elements are present: (i) coercion by one state of another state; and (ii) in relation to "matters in which each state is permitted, by the principle of state sovereignty, to decide freely."[4] As regards what is encompassed by the latter element, the ICJ in the *Nicaragua* case provided specific examples such as the "choice of a political, economic, social and cultural system, and the formulation of foreign policy."[5] This is often referred to as the *domaine réservé* of a state.

9. In order for the principle to be engaged, an intervention in the cyber context must be of sufficient seriousness, comparable in scale and effects to coercive action in a non-cyber

[2] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [212].
[3] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [202]. The principle is also reflected in Article 2(7) of the UN Charter, which provides: "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII."
[4] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [205].
[5] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [177].

context. For instance, malicious cyber-operations seriously compromising healthcare systems or national elections are capable of amounting to unlawful interventions.

10. Unlawful interventions should be distinguished from lawful forms of influence and pressure on states, such as lobbying governments or unfriendly acts. Likewise, they do not include countermeasures permitted under international law to induce a state to comply with its obligations on foot of an internationally wrongful act.

Principle of Due Diligence

11. The principle of due diligence derives from the principle of sovereignty. International law requires that a state may not knowingly allow its territory to be used for acts contrary to the rights of other states.[6]

12. Ireland considers the due diligence principle to be a primary rule of international law. Therefore, a breach of this international obligation, which is attributable to a state, engages state responsibility. For instance, the ICJ in the *Corfu Channel* case held that "nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania".[7] Similarly, in the *Armed Activities on the Territory of the Congo* case*,* the ICJ found that Uganda was responsible "for any lack of vigilance preventing violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account".[8]

13. Due diligence is a standard of conduct and not of result. What the scope of the obligation might entail is context specific.[9] In the cyber context, the principle of due diligence requires at a minimum that a state take all measures that are feasible in the circumstances to put an end to cyber-operations conducted from its territory or by persons within its jurisdiction that affect a right of, and produce serious adverse consequences for, other states.[10] In determining what is feasible in the circumstances, relevant factors include the capacity of the state concerned, the seriousness of the operations as well as the extent to which the state concerned has knowledge of the operations. Ireland considers that constructive knowledge, often described as a situation where a state "ought to have been aware", is capable of satisfying the knowledge component of the obligation of due diligence where this can be ascertained to an appropriate level.

---

[6] *Corfu Channel Case (UK v Albania)* ICJ Reports 1949, p.22.
[7] *Corfu Channel,* p.23.
[8] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, ICJ Reports 2005, p. 168, [179].
[9] See: *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* Judgment (2007) ICJ Rep 43, [429].
[10] Tallinn Manual 2.0, Rule 7.

14. A preventive element to the obligation of due diligence also arises in the cyber context. While a state cannot be expected to monitor all ICT activities within its territory, where for example a state is aware of an identifiable risk that actors within its jurisdiction intend to conduct cyber activities that are potentially harmful to the rights of, and potentially produce serious adverse consequences for, another state, the due diligence obligation requires that reasonable and feasible measures are taken to prevent such activities or mitigate their effects.

15. Much of the consideration of the principle of due diligence in international law has been in the context of environmental obligations. While its application to cyber-operations seems clear as a general principle, its more precise parameters in this context might benefit from further consideration. For instance, in what circumstances constructive knowledge (as distinct from actual knowledge) might suffice to breach an obligation of due diligence in the cyber context, the standard to be applied in respect of constructive knowledge, as well as the scope of a preventive element to the due diligence obligation, are all matters on which there appears to be a lack of shared understanding among states.

Use of Force

16. Article 2(4) of the Charter of the United Nations prohibits the threat or use of force by states against the territorial integrity or political independence of any other state. The Charter sets out two exceptions to this prohibition, namely when force is authorised by the UN Security Council and when it is used in the exercise of individual or collective self-defence. At the OEWG, states reaffirmed that "international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment".[11]

17. The prohibition on the use of force applies regardless of the means or weapons employed.[12] In the *Nicaragua* case*,* looking at the notion of "force", the ICJ determined that assistance to rebels in the form of the provision of weapons or logistical or other support may be regarded as a threat or use of force.[13] The Court further determined that "scale and effects" are to be considered when determining whether particular actions amount to an "armed attack".[14]

[11] A/AC.290/2021/CRP.2, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, Final Substantive Report (10 March 2021), [34].
[12] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* International Court of Justice (ICJ), 8 July 1996*,* para. 39.
[13] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14 [228].
[14]*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [195].

18. In Ireland's view, a cyber-operation attributable to a state will amount to a use of force if its scale and effects correspond to those of a physical use of force. This may include instances where a cyber-operation does not cause physical damage, such as where there is significant impairment of functionality of critical infrastructure. It is recalled that treaties, including the UN Charter, must be interpreted in the light of their object and purpose.[15] Although present day technology and our heavily digitised world may not have been contemplated at the time of the adoption of the Charter, it is appropriate to interpret Article 2(4) as applying to force emanating from cyber operations, notwithstanding the fact that the traditional physical or kinetic element may be lacking in terms of both means and impact.

19. For completeness, it is noted that a cyber-operation that falls below the threshold of use of force might nonetheless constitute an unlawful intervention in the internal affairs of a state or a violation of its sovereignty. Moreover, not every use of force contrary to Article 2(4) will amount to an "armed attack" within the meaning of Article 51 of the UN Charter (this is considered further under the heading of self-defence, below).

Legal Attribution

20. It is an established principle of international law that every internationally wrongful act of a state entails responsibility. As set out in the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), there is an internationally wrongful act of a state when conduct consisting of an action or omission: first, is attributable to the state under international law; and secondly, constitutes a breach of an international obligation of the state.[16] While the ARSIWA are not legally binding, in most respects they are widely accepted as largely reflecting customary international law. Absent any rules constituting *lex specialis*, the general rules of state responsibility apply in the cyber context.

21. In customary international law, attribution of an internationally wrongful act to a state can arise in several situations including: acts of organs or officials of the state; *ultra vires* acts; acts of individuals if conduct is directed and controlled by the state; and acts of individuals whose conduct has been acknowledged or adopted by the state.[17] The last two scenarios are arguably the most relevant in the context of cyberspace, as the nature of cyber-operations means that they can be very difficult to attribute to a specific state organ or official directly.

22. In relation to the concepts of direction and control, in the *Nicaragua* case the ICJ determined that responsibility for the actions of a third party arose where there was "effective control of the military or paramilitary operations in the course of which the

[15] 1969 Vienna Convention on the Law of Treaties, Article 31.
[16] Article 2 ARSIWA.
[17] See Articles 4 to 11 ARSIWA

alleged violations were committed."[18] The ICJ confirmed the effective control test in the *Genocide Convention* case.

23. Article 11 ARSIWA states that "conduct which is not attributable to a state under the preceding articles shall nevertheless be considered an act of that state under international law if and to the extent that the state acknowledges and adopts the conduct in question as its own." In the *Tehran Hostages* case, the ICJ held that state responsibility was engaged with what the Court called, "the seal of official government approval".[19] In a cyber context, a malicious cyber-operation conducted by a third party can thus be attributed to a state where it essentially takes ownership of the act, which might be ascertained through acts of support, approval and/or acquiescence.

24. There is a distinction to be drawn between legal attribution and political attribution. The former is a strictly legal exercise grounded in international law and the rules of state responsibility, while the latter is likely to be informed by political and technical assessments, often heavily based on intelligence reports. It is important to maintain clarity between the different frameworks in which legal attribution and political attribution are to be considered.

Countermeasures

25. Under well-established rules of state responsibility, a state responsible for an internationally wrongful act is under an obligation to cease its behaviour and to make full reparation for the injury caused. A state that is the victim of a cyber-operation constituting an internationally wrongful act attributable to another state may respond in various ways, including seeking recourse through dispute resolution mechanisms, where available. Recourse to countermeasures – *i.e.* measures which would otherwise be unlawful – against the state responsible for the internationally wrongful act to induce compliance is permitted in accordance with the limitations imposed by international law. Countermeasures must *inter alia* be proportionate and temporary in character and cannot include the use of force. There is no requirement for responsive measures to be similar in kind and in this context therefore they may include non-cyber means.

26. On the question of third party or collective countermeasures, Ireland considers that since the adoption of the ARSIWA in 2001, state practice indicates that such measures are permissible in limited circumstances, in particular in the context of violations of peremptory norms. The possibility of imposing third party or collective countermeasures in the cyber context is particularly relevant for states that may consider it necessary to respond to a malicious cyber-operation with a counter-operation, but lack the technological capacity to do so on their own.

---

[18] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986, p. 14, [86] [109] and [115].

[19] *United States Diplomatic and Consular Staff in Tehran*, Judgment, ICJ Reports 1980, p. 3, [73].

Self-Defence

27. The customary international law right to self-defence is acknowledged in Article 51 of the UN Charter, which states: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." States can invoke the right to self-defence in response to an "armed attack". Not every threat or use of force within the meaning of Article 2(4) of the Charter will amount to an armed attack and it is necessary to consider scale and effects.[20]

28. A cyber-operation that by virtue of its scale and effects reaches the threshold of an armed attack would permit the exercise of self-defence in accordance with Article 51 and customary international law. Due to the nature of a cyber-operation, it seems that only in exceptional circumstances could it reach the threshold of "armed attack". To reach this threshold, the scale and effects of a cyber-operation must correspond to an armed attack involving a physical use of force. It is conceivable that this need not necessitate physical damage, where for example loss or impairment of functionality to ICT infrastructure is inflicted on such a scale and with such effects that it is comparable to a conventional armed attack.

International Humanitarian Law

29. International humanitarian law (IHL) applies in situations of armed conflict (international or non-international). Cyber operations that take place in the context of, or themselves amount to, an armed conflict are regulated by IHL, including the principles of humanity, necessity, proportionality and distinction. States, through the GGE, have acknowledged the relevance of these key IHL principles to the use of ICTs by states.[21]

30. Cyber operations that have similar effects to physical military operations constituting armed force will bring into existence an international armed conflict if conducted between states, and can bring into existence a non-international armed conflict if the usual criteria are satisfied, namely that the violence has reached the requisite level of intensity and that it is between at least two organised parties.

31. The concept of an "attack" in IHL encompasses cyber operations expected to cause death, injury or physical damage. In Ireland's view it also extends to cyber operations expected to cause loss of functionality to networks or electronic systems. To interpret the term otherwise would mean that a cyber-operation that is directed at making a civilian network (such as electricity, banking, or communications) dysfunctional, or is expected

[20] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* Merits Judgment, ICJ Reports 1986.
[21] A/70/174 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report (22 July 2015), [28(d)].

to cause such effect incidentally, might not be covered by essential IHL rules protecting civilians and civilian objects,[22] and would not be consistent with the object and purpose of the Geneva Conventions and their Additional Protocols.

32. Ireland strongly disagrees with any suggestion that affirming the application of IHL to cyberspace encourages or legitimises the militarisation of cyberspace. IHL is concerned with limiting the suffering caused by armed conflict and mitigating its effects, rather than with the justifiability of the initiation of the conflict.

International Human Rights Law

33. States are bound by international human rights law in respect of activities in cyberspace. The same rights that individuals enjoy offline must be protected online.[23] This includes international and regional human rights treaties as well as customary international law. It is noted in particular that the foremost global human rights instrument, the International Covenant on Civil and Political Rights, applies to all individuals within a state party's territory and subject to its jurisdiction.[24]

34. Ireland considers an open, stable, accessible and safe internet to be an essential foundation for the protection of international human rights law in cyberspace. Any restrictions imposed by states on human rights in a cyber context must fall within parameters recognised as permissible under international human rights law. State sovereignty cannot be relied on as a guise for censoring free internet or otherwise impinging on applicable human rights. Any exercise of state sovereignty must be consistent with international human rights law.

Dublin

July 2023

[22] ICRC Position Paper, "International Humanitarian law and Cyber Operations during Armed Conflicts" (November 2019), p.8.
[23] Human Rights Council Resolution 20/8.
[24] International Covenant on Civil and Political Rights, Article 2.