The Application of International Law to State Activity in Cyberspace

NEW ZEALAND

Introduction

1. New Zealand supports an international rules-based system that promotes an open, secure, stable, accessible and peaceful online environment and encourages responsible state behaviour in cyberspace.
2. Recent advances in cyber capability and a rise in malicious activity online raise novel questions about how international law applies to state activity in cyberspace. These questions have been considered in a number of contexts, including by states, by the *United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* (and its precursors), by the *United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, and by experts, including in the *Tallinn Manual* process and through a series of *Oxford Statements on International Law Protections*. In order to facilitate broader and deeper consensus on these issues, this statement sets out New Zealand's position on how international law applies to state activity in cyberspace.

International law applies online as it does offline

3. International law applies online as it does offline. Applicable international law includes: the United Nations Charter; the law of state responsibility; international humanitarian law; and international human rights law.
4. While there is consensus amongst states that international law applies to state activity in cyberspace, the question of *how* it applies is nuanced. Activities in cyberspace involve, at least:
    a. A human component: the real people operating in the physical world, some of whom may be state agents or acting on the instructions of, or under the direction or control of, a state, and who use and misuse information and communications technology (ICT).
    b. A tangible, physical component: the cyber infrastructure and hardware physically located in the sovereign territory of a state.
    c. An intangible, virtual component: the data, operating systems, software, information and content of cyberspace. These elements can operate with a transboundary character, including through cyber personas.
5. As international law has evolved primarily with a territorial, physical conception of the world, care is required to apply the established rules and principles of international law appropriately to the multi-layered context of cyberspace. Applied appropriately, existing international law – as part of the framework of responsible state behaviour in cyberspace – provides an effective toolkit to regulate state behaviour online. This includes the ability to identify breaches of international law in cyberspace, attribute state responsibility for those breaches, and guide responses from victim states.

Use of Force

6. The United Nations Charter and customary international law rules concerning the use of force apply to state activity in cyberspace. Relevant obligations include:
    a. the requirement to settle disputes by peaceful means;
    b. the prohibition on the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations ; and
    c. the right of self-defence against an imminent or ongoing armed attack.
7. State cyber activity can amount to a use of force for the purposes of international law. Whether it does in any given context depends on an assessment of the scale and effects of the activity. State cyber activity will amount to a use of force if it results in effects of a scale and nature equivalent to those caused by kinetic activity which

constitutes a use of force at international law. Such effects may include death, serious injury to persons, or significant damage to the victim state's objects and/or state functioning. In assessing the scale and effects of malicious state cyber activity, states may take into account both the immediate impacts and the intended or reasonably expected consequential impacts.

8. Cyber activity that amounts to a use of force will also constitute an armed attack for the purposes of Article 51 of the UN Charter if it results in effects of a scale and nature equivalent to those caused by a kinetic armed attack. As an example, cyber activity that disables the cooling process in a nuclear reactor, resulting in serious damage and loss of life, would constitute an armed attack.

Non-intervention

9. Malicious state cyber activity may be inconsistent with the rule of non-intervention. Such activity will violate the rule of non-intervention if it:
    a. has significant effects on a matter which falls within the target state's inherently sovereign functions / *domaine réservé* (e.g. the right freely to choose its political, economic, social and cultural system, or matters such as taxation, national security, policing, border control, and the formulation of foreign policy); and
    b. is coercive (i.e. there is an intention to deprive the target state of control over matters falling within the scope of its inherently sovereign functions). Coercion can be direct or indirect and may range from dictatorial threats to more subtle means of control. While the coercive intention of the state actor is a critical element of the rule, intention may in some circumstances be inferred from the effects of cyber activity.
10. Examples of malicious cyber activity that might violate the non-intervention rule include: a cyber operation that deliberately manipulates the vote tally in an election or deprives a significant part of the electorate of the ability to vote; a prolonged and coordinated cyber disinformation operation that significantly undermines a state's public health efforts during a pandemic; and cyber activity deliberately causing significant damage to, or loss of functionality in, a state's critical infrastructure, including – for example – its healthcare system, financial system, or its electricity or telecommunications network.

Sovereignty

11. The principle of sovereignty prohibits the interference by one state in the inherently governmental functions of another and prohibits the exercise of state power or authority on the territory of another state. In the physical realm, the principle has legal effect through the prohibition on the use of force, through the rule of non-intervention and also through a standalone rule of territorial sovereignty. Subject to limited exceptions (e.g. authorisation by the United Nations Security Council, self-defence, consent), that standalone rule prohibits a state from sending its troops or police forces into or through, or its aircraft over, foreign territory, and prohibits a state from carrying out official investigations or otherwise exercising jurisdiction on foreign territory.
12. In the cyber realm, the principle of sovereignty is given effect through the prohibition on the use of force and the rule of non-intervention. New Zealand considers that the standalone rule of territorial sovereignty also applies in the cyber context but acknowledges that further state practice is required for the precise boundaries of its application to crystallise.
13. In New Zealand's view, the application of the rule of territorial sovereignty in cyberspace must take into account some critical features that distinguish cyberspace from the physical realm. In particular: i) cyberspace contains a virtual element which has no clear territorial link; ii) cyber activity may involve cyber infrastructure operating simultaneously in multiple territories and diffuse jurisdictions; and iii) the lack of physical distance in cyberspace means malicious actors can apply instantaneous effects on targets without warning. These features present unique opportunities for malicious actors and significant defensive challenges for states. They also make it difficult for states to prevent malicious cyber activity being conducted from or routed through their territory.
14. Bearing those factors in mind, and having regard to developing state practice, New Zealand considers that territorial sovereignty prohibits states from using cyber means to cause significant harmful effects manifesting on the territory of another state. However, New Zealand does not consider that territorial sovereignty prohibits

every unauthorised intrusion into a foreign ICT system or prohibits all cyber activity which has effects on the territory of another state. There is a range of circumstances – in addition to pure espionage activity – in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful. For example, New Zealand considers that the rule of territorial sovereignty as applied in the cyber context does not prohibit states from taking necessary measures, with minimally destructive effects, to defend against the harmful activity of malicious cyber actors.

15. A detailed factual enquiry is required in each case to determine whether state cyber activity that has effects manifesting on the territory of another state, but which does not amount to a use of force or a prohibited intervention, nonetheless involves a violation of the standalone rule of territorial sovereignty. That factual enquiry should take into account the scale and significance of the effects, the objective of the activity, and the nature of the target.

Due Diligence

16. An agreed norm of responsible state behaviour provides that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Whether this norm also reflects a binding legal obligation is not settled. Some states consider that, subject to certain knowledge and capacity requirements, customary international law requires states to take reasonable measures to put an end to malicious cyber activity which is conducted from, or routed through, their territory, if the activity is contrary to the rights of another state.

17. New Zealand is not yet convinced that a cyber-specific "due diligence" obligation has crystallised in international law. It is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders. If a legally binding due diligence obligation were to apply to cyber activities, New Zealand considers it should apply only where states have actual, rather than constructive, knowledge of the malicious activity, and should only require states to take reasonable steps within their capacity to bring the activity to an end.

Responding to Malicious Cyber Activity

18. Regardless of whether the activity amounts to an internationally wrongful act, a state may always attribute *political* responsibility for malicious state cyber activity and may always respond with retorsion (i.e. unfriendly acts not inconsistent with international law).

19. Where a state is subject to cyber activity that amounts to an internationally wrongful act, it may also invoke the international *legal* responsibility of the responsible state. States are responsible for internationally wrongful acts that can be attributed to them, including wrongful cyber activities. An internationally wrongful act can be attributed to a state if it was carried out by organs of the state, persons or entities empowered to exercise elements of governmental authority on behalf of that state, or agents acting on the instructions of, or under the direction or control of the state; or where the state acknowledges and adopts the act as its own. States may also be internationally responsible for aiding or assisting internationally wrongful cyber activity carried out by another state.

20. States should act in good faith and take care when attributing legal responsibility to another state for malicious cyber activity. While international law prescribes no clear evidential standard for attributing legal responsibility for internationally wrongful acts, a victim state must be sufficiently confident of the identity of the state responsible. What constitutes sufficient confidence in any case will depend on the facts and nature of the activity. While any legal attribution should be underpinned by a sound evidential basis, there is no general obligation on the attributing state to disclose that basis. However, a state may choose as a matter of policy to disclose specific information that it considered in making its attribution decision, and may be required to defend any such decision as part of international legal proceedings.

21. If State A attributes internationally wrongful cyber activity to State B, State A may demand reparation and guarantees of non-repetition and/or utilise peaceful dispute resolution mechanisms, including the International Court of Justice where available. State A may also respond with countermeasures against State B. Countermeasures

are otherwise internationally wrongful acts that are permitted when undertaken to induce another state to comply with its obligations under international law. They may include, but are not limited to, cyber activities that would otherwise be prohibited by international law. Any countermeasure must:

a. be undertaken to induce compliance by the state in breach of international law;

b. be directed at the state responsible for the internationally wrongful act;

c. not rise to the level of use of force or breach peremptory norms of international law; and

d. be necessary and proportionate.

22. Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim states, New Zealand is open to the proposition that victim states, in limited circumstances, may request assistance from other states in applying proportionate countermeasures to induce compliance by the state acting in breach of international law. In those circumstances, collective countermeasures would be subject to the same limitations set out above.

23. Where malicious cyber activity gives rise to a situation leading to international friction or a dispute endangering the maintenance of peace and security, any UN Member State may bring the situation or dispute to the attention of the UN Security Council and/or General Assembly.

24. A state subjected to malicious cyber activity amounting to an armed attack has further recourse to the inherent right of individual and/or collective self-defence in accordance with Article 51 of the UN Charter. The right to self-defence also arises when an armed attack is imminent, including by cyber means. Any exercise of that right:

a. may include, but is not limited to, cyber activities; and

b. must be consistent with relevant UN Charter and customary international law obligations, including notification to the United Nations, necessity, and proportionality.

International Humanitarian Law

25. In situations of armed conflict, international humanitarian law applies to cyber activities. A cyber activity may constitute an "attack" for the purposes of international humanitarian law where it results in death, injury, or physical damage, including loss of functionality, equivalent to that caused by a kinetic attack. All cyber "attacks" must comply with the principles of military necessity, humanity, proportionality and distinction.

International Human Rights Law

26. International human rights law applies to cyber activities. States must comply with their obligations to protect and respect human rights online, including the right to freedom of expression and the right not to be subjected to arbitrary and unlawful interference with privacy. States are obliged to respect and ensure human rights to those individuals within their territory and subject to their jurisdiction. The circumstances in which states exercise jurisdiction, through cyber means, over individuals outside their territory is currently unsettled and would benefit from further discussion in multilateral fora.

1 December 2020

NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Manatū Aorere

Te Tari Ture o te Karauna
Crown Law