Australia Non Paper
Case studies on the application of international law in cyberspace

The international community recognises that existing international law – and in particular the UN Charter in its entirety – is applicable to state conduct in cyberspace and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. This is reflected in the 2013 and 2015 reports of the UN Group of Governmental Experts on the use of Information Communications Technologies in the Context of International Security (UNGGE),[1] as adopted by the UN General Assembly.[2] Australia's position on how international law governs state conduct in cyberspace is presented in the International Cyber Engagement Strategy (2017), Annex A,[3] as supplemented by the 2019 International Law Supplement.[4]

These case studies apply international law to standalone hypothetical scenarios, demonstrating that existing treaties and customary international law provide a comprehensive and robust framework to address the threats posed by state-generated or sponsored malicious cyber activity. In particular, international law provides victim states with a "tool kit" to identify breaches of international legal obligations, attribute those acts to the responsible state, seek peaceful resolution of disputes and, where the victim state deems appropriate, take lawful measures in response. The case studies illustrate that the application of existing international law to cyberspace can enhance international peace and security by increasing predictability of state behaviour, reducing the possibility of conflict, minimising escalation and preventing misattribution.

The case studies represent fictional scenarios and are not based on actual actors or events. They are intended to illustrate potential options rather than recommend a course of action. They do not purport to represent how Australia could or would respond to any malicious cyber activity directed against it, or purport to provide a comprehensive view on potential response options or the international law issues raised in any specific scenario.

[1] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013) UN Doc A/68/98 para 19; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174 para. 24.
[2] UNGA Resolution 68/243 (9 January 2014) UN Doc A/RES/68/243; UNGA Resolution 70/237 (30 December 2015) UN Doc A/RES/70/237.
[3] Available at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/annexes.html#Annex-A and also enclosed at **Attachment 1**
[4] Available at https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_international_law_supplement.html and also enclosed at **Attachment 2**

Scenario 1 – Cyber operations by State B on government systems and websites of State A

State A undertakes major reforms to its domestic company law and tax code that are consistent with its international obligations. In order to implement the new laws – including to allow State A's tax office and corporate regulator to monitor and enforce new requirements on companies – State A requires all registered companies to disclose certain information via a government website. State B opposes the reforms because it considers they unfairly impact on the interests of companies from State B operating in State A. In an attempt to prevent State A from implementing the reforms, State B, through its Department of Defence, conducts a series of cyber operations that prevent use of the website and disable government systems of State A's tax office and corporate regulator. As a result, State A is incapable of regulating companies' compliance with the new laws for a substantial period and has no choice but to indefinitely postpone implementation of the new tax reforms. State A also loses significant tax revenue.

International law may assist State A in the following ways:

First, it provides **rules of legal attribution** – contained in the customary international law on state responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts – meaning that acts of the Department of Defence, as an organ of State B, would be attributable to State B.

Second, it **defines states' rights and obligations**, including the international law duty not to intervene in the internal affairs of another state (prohibited intervention). State B's conduct could constitute a prohibited intervention on the basis that it was a coercive interference in matters which State A is entitled as a matter of state sovereignty to decide freely, including its economic system. However, establishing the aforementioned elements of prohibited intervention would depend on the circumstances, including the extent of economic damage and the loss of government control over economic policy.

Third, if State B's conduct violated international law, it would entitle State A to **invoke the international legal responsibility** of State B, and State A could demand that State B cease the unlawful act/s (if they were continuing) and make full reparation for State A's injuries. Reparation could include restoring full access to relevant websites and providing compensation for any financially assessable damage. As international law governs the dispute, State A may seek to pursue resolution through legal as well as political avenues including, for example, by seeking a resolution consistent with the Charter of the United Nations, including Chapter VI (*Pacific Settlement of Disputes*),[5] which could include referring the dispute to the International Court of Justice (ICJ) where the necessary preconditions had been met (including admissibility and jurisdiction).

[5] For example: Article 33(1) of the UN Charter provides that "The parties to any dispute, the continuance of which is likely to endanger the maintenance of international peace and security, 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." In *Security Our Common Future: An Agenda for Disarmament* (Office for Disarmament Affairs, 2018) the UN Secretary-General commits to "make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace".

Fourth, if State B's conduct violated international law, it would entitle State A to take **countermeasures** – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as temporarily not performing certain bilateral treaty obligations owed to State B. However, State A would need to ensure that such countermeasures:

- were directed against State B
- *did not* constitute a threat or use of force, violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms
- were reversible (as far as possible)
- were proportionate to the injury suffered by State A, and
- were intended to induce State B to comply with its international legal obligations.

International law would not preclude State A from taking **acts of retorsion**, which are unfriendly acts that are not inconsistent with the international obligations of State A, including, for example, declaring diplomats from State B in State A *persona non grata*.

Scenario 2 – State A's territory/infrastructure used by State B to conduct malicious cyber activities against State C

State B's Department of Defence conducts malicious cyber activities against State C that are routed through servers located on State A's territory, without its knowledge. The malicious cyber activities conducted by State B are contrary to the rights of State C (although they do not constitute an unlawful use of force). State A's relationship with State C could be damaged.

International law may assist State A in the following ways:

> *First*, it provides **rules of legal attribution**, under which the unlawful acts of State B could not be attributed to State A. The rules of attribution (as outlined in Scenario 1) provide a clear legal framework for connecting the conduct of an individual or an entity to a state; this connection would not be established in the present case between State B's Department of Defence and State A. Rather, the acts of the Department of Defence would be attributable to State B as an organ of that state exercising executive functions. Attribution would also be made out against State B if it used a proxy acting on its instructions, or under its direction or control, to carry out the relevant acts. Additionally, State A would not be considered responsible for aiding and assisting State B because its lack of knowledge of the wrongful acts and its lack of intent to aid or assist the wrongful acts would mean that it could not have been complicit in the commission of those acts. Therefore, State C could not make a legal attribution of the wrongful conduct to State A.
>
> *Second*, as a result, State A **could not be considered directly responsible for any unlawful act** committed by State B against State C. Accordingly, State C could not pursue dispute resolution through legal avenues (including the ICJ, as outlined in Scenario 1) against State A in relation to State B's wrongdoing; although it could do so against State B. Additionally, assuming State A could not have been aware of the activity taking place from its territory, it did not act contrary to the norm of responsible state behaviour in cyberspace to not knowingly allow its territory to be used for internationally wrongful acts using ICTs,[6] or in violation of any applicable international obligations.
>
> *Third*, as State A is not directly responsible for any unlawful act committed by State B against State C, State C could not take any **countermeasures** – acts that would ordinarily be unlawful – against State A in response to State B's conduct. Were it to do so, State A would itself be entitled to respond through countermeasures and seek remedies.

Note: this scenario details how international law would assist State A (whose territory/infrastructure was used without its knowledge by State B to conduct malicious activity against State C). Separately, and provided all requirements were met (see Scenario 1), State C could invoke the international legal responsibility of State B and pursue a legal and/or political resolution and take countermeasures and/or acts of retorsion against it.

[6] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015) UN Doc A/70/174 para. 13(c) (see, also, para. 13(h)).

Scenario 3 – State B conducts a major offensive cyber operation that constitutes a serious threat to State A's national security

Amid growing tensions between State A and State B,[7] the armed forces of State B conduct a major offensive cyber operation against State A, destroying servers located in State A used by State A's military headquarters. This renders State A unable to communicate with naval vessels operating in international waters off the coast of State B. It will take several months to replace the destroyed servers, at substantial cost.

International law may assist State A in the following ways:

First, it provides **rules of legal attribution**, meaning that under the customary international law on state responsibility (as outlined in Scenario 1), the acts of the armed forces, as an organ of State B, would be attributable to State B.

Second, it **defines states' rights and obligations**, meaning that State B's cyber operation may constitute an unlawful use of force contrary to Article 2(4) of the UN Charter against State A (unless such actions were taken in self-defence or authorised under a Chapter VII resolution of the UN Security Council). This would turn on whether the operation caused damage to State A's infrastructure and objects (its military servers) and subsequent impact on the functioning of its military communications systems that was akin in scale and effects to a traditional kinetic operation that would rise to the level of a use of force.

Third, assuming State B's conduct violated international law, it would entitle State A to **invoke the international legal responsibility** of State B and demand that State B cease unlawful act/s (if they were continuing) and make full reparation for State A's injuries. Reparation could entail compensation for financially assessable damage, as well as assurances or guarantees of non-repetition. As international law governs the dispute, State A may seek to pursue resolution through legal as well as political avenues including, for example, by seeking a resolution consistent with the Charter of the United Nations, including Chapter VI (*Pacific Settlement of Disputes*) [8] (which could include the International Court of Justice, as outlined in Scenario 1) and/or Chapter VII (*Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*)[9].

[7] For the purposes of this scenario, there is not a state of armed conflict between State A and State B immediately prior to State B's offensive cyber operation.
[8] See note 5 above.
[9] For example: Article 39 of the UN Charter provides that "The [UN] **Security Council** shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42 to maintain or restore international peace and security."

Fourth, if State B's conduct violated international law, it would entitle State A to take **countermeasures** – acts which would ordinarily be unlawful – in response to State B's wrongdoing. Countermeasures could be cyber in nature or taken through alternative means – such as implementing otherwise unlawful tariffs on trade in important goods/services from State B. However, State A would need to ensure that such countermeasures:

- were directed against State B
- *did not* constitute a threat or use of force, violate fundamental human rights, humanitarian obligations prohibiting reprisals, or peremptory international legal norms
- were reversible (as far as possible)
- were proportionate to the injury suffered by State A, and
- were intended to induce State B to comply with its international legal obligations.

Fifth, if the cyber operation constituted an "armed attack", as recognised under Article 51 of the UN Charter, State A would be entitled to use force pursuant to its inherent right of **self-defence** against State B. The use of force in self-defence may be cyber in nature or conducted through kinetic means. However, the right to self-defence would require that State A only use force where it is necessary to repel the actual or imminent armed attack and that such force be a proportionate response in scope, scale and duration. The measures taken by State A would need to be immediately reported to the UN Security Council.

International law would not preclude State A from taking **acts of retorsion**, which are unfriendly acts that are not inconsistent with the international obligations of State A, including, for example, declaring diplomats from State B in State A *persona non grata*.

ATTACHMENT 1

2017 - AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

Existing international law provides the framework for state behaviour in cyberspace. This includes, where applicable, the law regarding the use of force, international humanitarian law (IHL), international human rights law, and international law regarding state responsibility.

In this respect, Australia notes that the centrality of international law and its application to states' use of cyberspace was affirmed in 2013 in the consensus report of the third *United Nations Group of Governmental Experts (UNGGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, which was chaired by Australia, and reaffirmed in the 2015 report of the UNGGE.

However, Australia recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty, attribution and jurisdiction, given that different actors engage in a range of cyber activities which may cross multiple national borders. This annex sets out Australia's views on these issues.

1. The United Nations Charter and the law on the use of force (*jus ad bellum*) apply to activities conducted in cyberspace.

The Charter of the United Nations requires states to seek peaceful settlements of disputes. This obligation extends to cyberspace and requires states to resolve cyber incidents peacefully without escalation or resort to the threat or use of force. This requirement does not impinge upon a state's inherent right to act in individual or collective self-defence in response to an armed attack, which applies equally in the cyber domain as it does in the physical realm.

In determining whether a cyber attack, or any other cyber activity, constitutes a use of force, states should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law. This involves a consideration of the intended or reasonably expected direct and indirect consequences of the cyber attack, including for example whether the cyber activity could reasonably be expected to cause serious or extensive ('scale') damage or destruction ('effects') to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.

2. For cyber operations constituting or occurring within the context of an international or non-international armed conflict, the relevant international humanitarian law (*jus in bello*) will apply to the conduct of these cyber activities.

International humanitarian law (IHL) (including the principles of humanity, necessity, proportionality and distinction) applies to cyber operations within an armed conflict.

The IHL principle of proportionality prohibits the launching of an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

The IHL principle of military necessity states that a combatant is justified in using those measures, not forbidden by international law, which are indispensable for securing complete submission of an enemy at the soonest moment. The principle cannot be used to justify actions prohibited by law, as the means to achieve victory are not unlimited.

The IHL principle of distinction seeks to ensure that only legitimate military objects are attacked. Distinction has two components. The first, relating to personnel, seeks to maintain the distinction between combatants and non-combatants or military and civilian personnel. The second component distinguishes between legitimate military targets and civilian objects.

All Australian military capabilities are employed in line with approved targeting procedures. Cyber operations are no different. Australian targeting procedures comply with the requirements of IHL and trained legal officers provide decision-makers with advice to ensure that Australia satisfies its obligations under international law and its domestic legal requirements.

For example, Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack under IHL', the rules governing such attacks during armed conflict will apply to those kinds of cyber operations.

3. For cyber activities taking place outside of armed conflict, general principles of international law, including the law on state responsibility, apply.
It is a longstanding rule of international law that, if a state acts in violation of an international obligation, and that violation is attributable to the state, that state will be responsible for the violation.

The customary international law on state responsibility, much of which is reflected in the International Law Commission's *Articles on the Responsibility of States for Internationally Wrongful Acts*, apply to state behaviour in cyberspace.

To the extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding responsibilities to ensure those objects and activities are not used to harm other states. In this context, we note it may not be reasonable to expect (or even possible for) a state to prevent all malicious use of ICT infrastructure located within its territory. However, in Australia's view, if a state is aware of an internationally wrongful act originating from or routed through its territory, and it has the ability to put an end to the harmful activity, that state should take reasonable steps to do so consistent with international law.

If a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures against the perpetrator state, under certain circumstances. However, countermeasures that amount to a use of force are not permissible. Any use of countermeasures involving cyberspace must be proportionate. It is acknowledged that this raises challenges in identifying and assessing direct and indirect effects of malicious cyber activity, in order to gauge a proportionate response. The purpose of countermeasures is to compel the other party to desist in the ongoing unlawful conduct.

ATTACHMENT 2

2019 - SUPPLEMENT TO AUSTRALIA'S POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO STATE CONDUCT IN CYBERSPACE

In the *International Cyber Engagement Strategy* (2017) (Strategy), Australia committed to periodically publish its position on the application of relevant international law to state conduct in cyberspace. The first such publication appeared in Annex A to the Strategy. This document is the second publication and is aimed at further elaborating Australia's position on applicable international law as expressed in the Strategy. As such, it should be read as a supplement to that document.

Application and development of international law

The Strategy recognised the well-established position that existing international law - including the UN Charter in its entirety - provides the framework for responsible state behaviour in cyberspace. The international community, including the permanent members of the United Nations (UN) Security Council recognised this in the 2013 and 2015 reports of the UN Group of Governmental Experts on the use of Information Communications Technologies in the Context of International Security (UNGGE), as adopted by the UN General Assembly. Australia also acknowledged that activities conducted in cyberspace raise new challenges for how international law applies. To deepen understandings and set clear expectations, Australia encourages states to be transparent in how they interpret existing international law as it applies to state conduct in cyberspace. The Strategy, and this supplement, form part of Australia's ongoing effort to make its views on the applicability of international law public.

The law on the use of force (jus ad bellum) and the principle of non-intervention

The United Nations Charter (Charter) and associated rules of customary international law apply to activities conducted in cyberspace. Article 2(3) of the Charter requires states to seek the peaceful settlement of disputes and Article 2(4) prohibits the threat or use of force by a state against the territorial integrity or political independence of another state, or in any manner inconsistent with the purposes of the UN. In the Strategy, Australia made clear that these obligations – and the UN Charter in its entirety, including those obligations, apply in cyberspace as they do in the physical realm.

A use of force will be lawful when the territorial state consents, it is authorised by the Security Council under Chapter VII of the UN Charter or when it is taken pursuant to a state's inherent right of individual or collective self-defence in response to an armed attack, as recognised in Article 51 of the Charter. Australia considers that the thresholds and limitations governing the exercise of self-defence under Article 51 apply in respect of cyber operations that constitute an armed attack and in respect of acts of self- defence that are carried out by cyber means. Thus if a cyber operation – alone or in combination with a physical operation – results in, or presents an imminent threat of, damage equivalent to a traditional armed attack, then the inherent right to self-defence is engaged. The rapidity of cyber attacks, as well as their potentially concealed and/or indiscriminate character, raises new challenges for the application of established principles. These challenges have been raised by Australia in explaining its position on the concept of imminence and the right of self-defence in the context of national security threats that have evolved as a result of technological advances (see Figure 1).

FIGURE 1 – IMMINENCE AND CYBER OPERATIONS

"[A] state may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.

This standard reflects the nature of contemporary threats, as well as the means of attack that hostile parties might deploy.

Consider, for example, a threatened armed attack in the form of an offensive cyber operation (and, of course, when I say 'armed attack', I mean that term in the strict sense of Article 51 of the Charter). The cyber operation could cause large-scale loss of human life and damage to critical infrastructure. Such an attack might be launched in a split-second. Is it seriously to be suggested that a state has no right to take action before that split-second?"

Attorney-General, Senator the Hon. George Brandis QC,
University of Queensland, 11 April 2017

Harmful conduct in cyberspace that does not constitute a use of force may still constitute a breach of the duty not to intervene in the internal or external affairs of another state. This obligation is encapsulated in Article 2(7) of the Charter and in customary international law. A prohibited intervention is one that interferes by coercive means (in the sense that they effectively deprive another state of the ability to control, decide upon or govern matters of an inherently sovereign nature), either directly or indirectly, in matters that a state is permitted by the principle of state sovereignty to decide freely. Such matters include a state's economic, political, and social systems, and foreign policy. Accordingly, as former UK Attorney-General Jeremy Wright outlined in 2018, the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems would constitute a violation of the principle of non-intervention.

International humanitarian law (*jus in bello*) and international human rights law

The Strategy and the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174), discussed the applicability of international humanitarian law (IHL) to cyber operations in armed conflict, including the principles of humanity, military necessity, proportionality and distinction. Australia considers that, if a cyber operation rises to the same threshold as that of a kinetic 'attack' (or act of violence) under IHL, the rules governing such attacks during armed conflict will apply to those kinds of cyber operations. Applicable IHL rules will also apply to cyber operations in an armed conflict that do not constitute or rise to the level of an 'attack', including the principle of military necessity and the general protections afforded to the civilian population and individual civilians with respect to military operations.

International human rights law (IHRL) also applies to the use of cyberspace (see e.g. Figure 2). States have obligations to protect relevant human rights of individuals under their jurisdiction, including the right to privacy, where those rights are exercised or realised through or in cyberspace. Subject to lawful derogations and limitations, states must ensure without distinction individuals' rights to privacy, freedom of expression and freedom of association online.

FIGURE 2 – COMMONWEALTH CYBER DECLARATION

"Recognising the potential for a free, open, inclusive and secure cyberspace to promote economic growth for all communities and to act as an enabler for realisation of the Sustainable Development Goals across the Commonwealth, we:
...

5. Affirm that the same rights that citizens have offline must also be protected online."

Commonwealth Heads of Government Declaration
20 April 2018

General principles of international law, including the law on state responsibility

In the Strategy, Australia recognised that the law on state responsibility, much of which is reflected in the International Law Commission's Articles on the Responsibility of states for Internationally Wrongful Acts, applies to state behaviour in cyberspace. Under the law on state responsibility, there will be an internationally wrongful act of a state when its conduct in cyberspace – whether by act or omission – is attributable to it and constitutes a breach of one of its international obligations.

Australia will, in its sole discretion, and based on its own judgement, attribute unlawful cyber operations to another state. In making such decisions, Australia relies on the assessments of its law enforcement and intelligence agencies, and consultations with its international partners (see e.g. Figure 3). A cyber operation will be attributable to a state under international law where, for example, the operation was conducted by an organ of the state; by persons or entities exercising elements of governmental authority; or by non-state actors operating under the direction or control of the state.

As outlined in the Strategy, if a state is a victim of malicious cyber activity which is attributable to a perpetrator state, the victim state may be able to take countermeasures (whether in cyberspace or through another means) against the perpetrator state, under certain circumstances. Countermeasures are measures, which would otherwise be unlawful, taken to secure cessation of, or reparation for, the other state's unlawful conduct. Countermeasures in cyberspace cannot amount to a use of force and must be proportionate. States are able to respond to other States' malicious activity with acts of retorsion, which are unfriendly acts that are not inconsistent with any of the State's international obligations.

If a state is the victim of harmful conduct in cyberspace, that state could be entitled to remedies in the form of restitution, compensation or satisfaction. In the cyber context, this may mean that the victim-state could for example seek replacement of damaged hardware or compensation for the foreseeable physical and financial losses resulting from the damage to servers, as well as assurances or guarantees of non-repetition.