ANNEX A

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.

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.