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.