Australia

EXECUTIVE SUMMARY

Australia welcomes the opportunity, in response to the invitation in General Assembly Resolution 70/237, to provide its views on developments in the field of information and telecommunications in the context of international security. This submission builds upon information provided by Australia in response to Res. 68/243 in 2014 and to Res. 65/41 in 2011.

Cyber security is as intrinsically linked to innovation as it is to national security. It is the bedrock of innovation, growth and prosperity. Cyber security is a global opportunity that governments, the private sector and the community are all invested in and can all derive benefit from.

The global community needs to get cyber security right. Everyone – governments, businesses and individuals – need to work together to build a trusted online environment. Not only to protect critical information, but to provide the environment for innovation to flourish; to enable the technology industry to thrive; and to capitalise on the growing global need for better cyber security solutions, equipment and skilled individuals.


Australia believes that a priority task for the international community is the elaboration of how international law applies to States’ behaviour in cyberspace especially in non-conflict situations. There is a need for further work to develop understandings on how key concepts such as sovereignty and jurisdiction apply in cyberspace, taking into account our common interest in preserving the global nature of the internet. There is scope for the further development of voluntary norms set out in the 2015 Report of the Group of Governmental Experts in relation to the protection of critical infrastructure, Computer Emergency Response Teams, the responsibility of States to assist, cooperation on cybercrime and preventing the proliferation of malicious cyber tools and techniques. It is important that work on confidence building measures moves to the next phase, from the promotion of transparency to the implementation of cooperative measures.

(a) General appreciation of the issues of information security

Australia prefers to use the term ‘cyber security’ rather than ‘information security’ because the latter is a source of possible confusion since some states regard information itself as a threat against which additional protection is required.

The internet and cyberspace are central to Australia’s national security and economic prosperity. Australia recognises strong cyber security as a fundamental element for growth and prosperity in a global economy. It is also vital for national security and requires partnership involving governments, the private sector and the community.

Being connected is now essential, creating new opportunities for innovation and growth for the global community. Australians have quickly embraced economic opportunities in cyberspace.
2014 alone, the Internet based economy contributed $79 billion to the Australian economy (or 5.1 per cent of GDP). This amount could grow to $139 billion annually (7.3 per cent of GDP) by 2020 as more devices, services and people are connected online.

As people and systems become increasingly connected, the quantity and value of information held online has increased. So have efforts to steal and exploit that information. Cyberspace, and the dynamic opportunities it offers, is under persistent threat.

Cyber threats are serious and growing in scale and sophistication and Australia is increasingly a target. Figures vary, but cybercrime is estimated to cost Australians over $1 billion each year and the full economic impact is estimated to be around $17 billion annually.

Australia recognises building a trusted online environment is essential for its future prosperity. Confidence in the security of its networks enables all individuals and organisations to do their business online securely. The global community – including governments, business and individuals – need to work together to build resilience to cyber security threats and to make the most of opportunities online.

**(b) Efforts taken at the national level to strengthen information security and promote international cooperation in the field**

i. **National efforts**

Australia’s cyber security is built on a solid foundation. Australia’s new Cyber Security Strategy, launched on 21 April 2016, answers the call for national leadership on cyber security, and provides a foundation for Australia’s future online prosperity. This Strategy establishes five themes of action for Australia’s cyber security over the next four years to 2020:

- A national cyber partnership
- Strong cyber defences
- Global responsibility and influence
- Growth and innovation
- A cyber smart nation

The Cyber Security Strategy states that national co-leadership and cross sectoral partnerships are essential for strong cyber security. A range of initiatives in Australia’s Cyber Security Strategy will be co-designed between governments, the private sector and the research community.

The Strategy was underpinned by a Review led by the Department of the Prime Minister and Cabinet. The Department, through the new position of a Special Adviser on Cyber Security, will coordinate implementation of this Strategy for the Government, in its central responsibility for cyber security policy.
ii. **Promotion of international cooperation**

Cyber security is a critical issue for Australia’s international cooperation. Developing norms of state behaviour, the application of international law, internet governance and cyber innovation are regularly discussed in Australia’s engagement with other governments and organisations bilaterally and in regional and multilateral fora.

Under the Strategy, Australia will develop an international cyber engagement strategy and appoint an Ambassador for Cyber Affairs to lead Australia’s international cyber effort. The Ambassador will advocate for an open, free and secure internet based on Australia’s values of free speech, privacy and the rule of law. This role will include coordination of Australia’s cyber capacity building efforts in the Indo-Pacific region, continuing to advocate against state censorship of the internet and promoting Australia’s view that the opportunities provided by the internet should be available to all people.

International leadership enhances global cooperation and economic development by taking advantage of the opportunities presented by new technologies. In partnership with other countries, Australia already works to strengthen the foundations of international stability in cyberspace, develop cooperative partnerships and build cyber security capacity. Actions include:

- Australia chaired the United Nations Group of Governmental Experts in 2012-2013 that found existing obligations under international law apply to State behaviour in cyberspace. Australia will continue to contribute to this important stream of work as a member of the 2016-2017 Group of Governmental Experts.
- Australia has participated in the series of global conferences on cyberspace initiated in London in November 2011 and hosted most recently by the Netherlands in The Hague in April 2015. At that conference Australia joined the Global Forum on Cyber Expertise to help coordinate international cyber capacity building efforts.
- Australia has played an important role in raising awareness of the need for measures to reduce the risk of misperception, miscalculation and escalation arising from cyber incidents through the development of the ASEAN Regional Forum Work Plan on Security of and in the Use of ICTs adopted by Ministers in August 2015. Australia has also organised Workshops in the ARF to develop awareness of the importance of coordination and communication between government agencies, between technical and policy personnel and between governments in responding to cyber incidents and in preventing their escalation. We are taking forward work to develop an ARF directory of cyber points of contact as a practical measure to facilitate communication between states in preventing crises and in responding to significant cyber incidents.
- Australia has contributed to the cross-fertilisation of ideas on developing confidence building measures to reduce risk between regions, sharing the experience of the ASEAN Regional Forum in this field with partners in the Organisation for Security and Cooperation in Europe.
- Australia has supported the work of the ICT4Peace Foundation to raise awareness of cyber policy issues with diplomats and government officials, helping to deliver workshops in Singapore in October 2015 and Addis Ababa in February 2016.
In 2015, Australia joined the Freedom Online Coalition—a partnership of 29 governments working to advance Internet freedom.

The Australian Federal Police is working with policing agencies throughout the Indo-Pacific region on training and capacity building initiatives to counter cybercrime. For example, the Cyber Safety Pasifika initiative is a collaborative project between the Pacific Islands Chiefs of Police and the Australian Federal Police. It has now been launched in 14 Pacific Island countries and has trained 40 Pacific Island instructors to deliver cyber safety education in their own countries and mentoring support in other Pacific Island countries. Over 72,000 children and young people in the Pacific have now attended its education and awareness workshops.

In 2013, Australia joined the Council of Europe Convention on Cybercrime, otherwise known as the Budapest Convention.

Australia’s national Computer Emergency Response Team, CERT Australia, currently chairs the steering committee of APCERT, the Asia Pacific Computer Emergency Response Teams (comprising 28 teams from 20 economies across the region) and shares threat information with other response teams around the world.

The Attorney-General’s Department provides assistance to Pacific Island countries to reform their criminal justice frameworks to address cybercrime.

(c) The content of the concepts mentioned in paragraph 3 of the resolution

Australia has consistently advocated for an open, free and secure cyberspace based on its values of freedom of speech, right to privacy and the rule of law. The multi-stakeholder model of internet governance, involving the private sector and the community as equal partners with government is the most effective model. It delivers economic benefit and social opportunity, and protects fundamental rights and freedoms.

Australia’s view is that international law provides the framework for state behaviour in cyberspace, and for appropriate responses to unlawful online activity pursued by states. This includes where applicable, international humanitarian law, law regarding the use of force, international human rights law and international law regarding state responsibility. Any measures used by States to deter and respond to malicious cyber activities should be consistent with the rules-based international order and the obligations of States under international law.

International law also provides the framework for the development of additional voluntary norms of state behaviour. Practical confidence building measures to reduce the risk of misperception, miscalculation and conflict, while addressing an immediate and urgent need, may overtime, as state practice, provide the basis for norms. In October 2015 Australia endorsed the consensus report of 2014-2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174). Australia joined the consensus on General Assembly Res. 70/237 in which member states agreed to be guided in their use of information and communications technologies by the 2015 UNGGE Report.

Australia, along with other members of the G-20, has affirmed that no country should conduct or support cyber-enabled theft of intellectual property, including trade secrets or other confidential
business information, with the intent of providing competitive advantages to companies or commercial sectors.

(d) Possible measures that could be taken by the international community to strengthen information security at the global level

Australia believes that a priority task for the international community is the continuing elaboration of how international law applies to States’ behaviour in cyberspace especially in non-conflict situations. The 2015 UNGGE Report, which set out additional norms, rules and principles for responsible State behaviour, provides an important and useful starting point for further work.

In relation to international law, the application and delineation of the fundamental concepts of sovereignty and jurisdiction requires further work. This work should take into account our common interest in preserving the global nature of the internet and obligations to uphold and protect universal human rights.

In relation to voluntary norms further work could include:

- Identifying and harmonising understanding between States as to which critical infrastructure sectors and associated information systems are most at risk.
- Development of understandings and the implementation of measures to prevent the proliferation of malicious ICT tools and techniques.
- The elaboration of the essential characteristics of a computer emergency response team qualifying for protection under the norm against harming such teams.
- Further elaboration of the norm involving the responsibility of states to respond to requests for assistance.
- Identifying strategies to prevent the cyber-enabled theft of intellectual property for commercial gain.

In relation to confidence building measures, there is a need to move from the promotion of transparency to the development and implementation of cooperative measures. Such measures should be implemented bilaterally, by small groups of states, and through regional security organisations. There is a need to integrate mechanisms for responding to cyber incidents, and for preventing their escalation, with national crisis management machinery. Exercising this machinery is critical to the development of capacity by governments, working together, to respond effectively. Measures to enable joint or small group exercising, such as harmonising the points at which countries escalate their management of routine cyber incidents to an issue of national security concern, or developing directories of points of contact covering policy and technical personnel, could be designed and implemented.