UNGA69 First Committee
28 October 2014

Thematic Statement: Other Disarmament Measures and International Security

Delivered by Ambassador John Quinn, Australian Permanent Representative to the United Nations, Geneva and Ambassador for Disarmament

Mr Chairman,

Australia welcomes a measured discussion in this committee about the international security implications of fast moving developments in cyberspace. It is appropriate that the United Nations should take the lead on consideration of this particular subject.

The internet now constitutes critical global infrastructure on which the broad international community – government, businesses, civil society, and individuals – all depend. The internet has empowered hundreds of millions of people round the globe to access all manner of opportunities. It also poses some novel and complex challenges with which governments, businesses and civil society are all grappling. This was well illustrated by the ground breaking Netmundial Conference in Sao Paolo earlier this year.

There is growing international attention to developing clearer rules of the road on what is acceptable behaviour in cyber space. Given the complexities involved, forging broad international agreement on such rules will necessarily be a longer term endeavour.

We have taken an important first step in this process – securing broad agreement that existing international law, including the UN Charter, applies to states’ conduct in cyberspace. This was the key conclusion of the
UNGGE consensus report adopted in June 2013 which Australia had the honour to chair, a conclusion which merits active reinforcement and promotion.

The next logical step is to give further consideration to how international law applies in cyber space. Australia remains fully committed to contributing to this work, on which a new UNGGE is now embarked. This discussion should go beyond focusing on armed conflict, and also address the question of State actions falling below the threshold of armed conflict and in peacetime.

There are now a myriad of actors and transactions in cyberspace where developments unfold rapidly. The risks of friction, unintended consequences and potentially serious conflict between states are thus very high, as are the stakes for the international community in avoiding such scenarios.

We have long experience with transparency and confidence building measures in the field of international security. TCBMs are a well-established way to address risks of misperception, misunderstanding and miscalculation, thus lowering risks of escalation that could lead to conflict. The 2013 UNGGE report endorses the value of this stream of work which is also being pursued in other contexts including the OSCE.

As a matter of urgency, specific TCBMs now need to be identified, elaborated, and agreed between states. And they also need to be put into practice and exercised. In this regard, Australia was pleased to co-chair with Malaysia a workshop on cyber confidence building measures in Kuala Lumpur in March this year under the auspices of the ASEAN Regional Forum. The centre-piece of this event was a very successful discussion exercise on how to de-escalate a major cyber incident in the financial sector which raised national, regional and international security considerations.

A key lesson from this workshop is the value of stronger regional and global networks of policy, technical/operational and other points of contact, including those at reasonably senior levels. Such networks should enable swift clarification to be sought from the country which appears to be the source of the cyber incident – preferably in a non-judgemental or accusatory fashion. There is also scope to develop clearer protocols between States, including in relation to what information can be sought through relevant channels.
Developing and elaborating TCBMs in the cyber domain will have direct and positive impact on regional and international security. Australia remains committed to working within the ASEAN Regional Forum and with other partners to advance this important agenda, recognising the particular mandate of such regional security bodies to build confidence and prevent conflict, and the value of sharing experiences between regions.

The 2013 UNGGE report also reaffirms the importance of capacity building. This subject is now an integral element of international cooperation on cyberspace. Australia is actively engaged in this field, especially in our region. We support innovative approaches to capacity building which reflect the fundamental multi-stakeholder dynamics of cyberspace, are based on sound assessments of needs and sustainability, and draw on international best practice.

In closing, we wish to acknowledge the important contribution made by the three international conferences held to date under the “London process” in advancing international cooperation in cyberspace in all its dimensions, including international security. We look forward to participating in the next such event – the Global Conference on Cyberspace 2015 to be hosted by the Netherlands in April 2015 – which will again bring together governments, the business community and civil society in productive dialogue.

Thank you, Mr Chairman.