Department of Foreign Affairs and Trade
RG Casey Building
John McEwen Crescent
Barton ACT 0221
Attn: Johanna Weaver

By Email: CyberAffairs@dfat.gov.au

Date 31 January 2020
Reference Responsible State Behaviour in Cyberspace in the Context of International Security at the United Nations

Internet Australia appreciates the opportunity to engage with the Department of Foreign Affairs on the issues involved in agreed norms of responsible state behaviour in cyberspace.

We commend the Australian government for conducting this public consultation and for providing the community with an opportunity to offer views on the implementation of agreed norms of responsible State behaviour in cyberspace. Internet Australia believes that this initiative is timely and that it will assume growing importance as the global economy and society become increasingly dependent upon a safe and well functioning internet which operates within a framework based upon the rule of law.

Internet Australia strongly supports the approach set out in the APNIC submission to this inquiry and shares APNIC's concern that International cybersecurity discussions amongst States at the UN may have been somewhat detached from technical considerations about the operation of networks. Because of this, there is a real danger that the processes for developing these norms have not reliably included technical knowledge or advice. Consequently, while some political objectives may have been reached, they are quite removed from the technical reality in which they exist.

In particular, we emphasize the critical nature of having appropriate private sector agencies and groups from the technical community involved in an on-going nature in future discussions aimed at promoting the development and promulgation of the UN Cyber Norms. These are the technical groups which develop and implement the standards under which the internet has been able to operate and to expand successfully over many years. Without such involvement, there is a very real danger that the Cyber Norms will lack practical application and will have little real impact.

Within the technical community, there are two important groups whose expertise in international cybersecurity is fundamental for the promotion of an "open, secure, stable, accessible and peaceful" cyberspace: the network operators and their Incident Response Teams, sometimes organised as internal or cooperative industry Computer Emergency Response Teams (CERTs). Both groups work mostly in the private sector and perform key functions in maintaining network operations and cooperating across political borders (including in times of conflict) for their security, stability and resilience.

We also wish to emphasise the importance of consumer perspectives within the development and promulgation of these norms. Within the considerations of governments, academics and commentators, cyber security is often discussed in terms of hacking attacks on government organizations, energy networks, defence agencies and large private corporations. An aspect of cybersecurity which is frequently overlooked is the impact which cyber incidents such as hacking and identity theft have on groups of individual consumers. These are the people whose identities are stolen, whose bank accounts are plundered, and who are frequently defrauded with little opportunity for effective redress. It is important that the interests of consumers be included in any discussions of global approaches to cyber norms, since it is individual consumers who bear the brunt of cyber incidents, notably identity theft.

A final general observation relates to the need for policy to be guided by a balance between the needs for effective and resilient cyber-security, and the clear need not to destroy individual privacy and freedom of choice in the process.

The events of Christchurch in March 2019 galvanised countries in Europe and Asia, including Australia, to call for urgent action and enhanced cooperation to address the increased threats of terrorist and violent extremist content online. But all such action:

> *…must be consistent with principles of a free, open and secure internet, without compromising human rights and fundamental freedoms, including freedom of expression. It must also recognise the internet's ability to act as a force for good, including by promoting innovation and economic development and fostering inclusive societies.*

The Australian Government has posed a series of questions relating to the cyber norms. Internet Australia has specific comments with regard to question five.

Internet Australia strongly supports and applauds the long-standing approach of successive Australian governments in pursuing sustained capacity building in a range of Asia/Pacific countries. This reflects a recognition that all sovereign nations need a base level of cyber security capacity if they are to play a responsible and supportive role in the growth of a safer internet. More importantly, the presence of sophisticated technology platforms in countries which have limited cyber detection and enforcement regimes lays open the clear, and often experienced danger of platforms in those countries being used for a wide range of criminal and other dangerous or questionable commercial activities. It is clearly in the interests of the global community for all nations to have in place basic levels of cyber detection, responsiveness and enforcement, backed up by appropriate legal regimes. Australia has long recognised this need and has been instrumental in encouraging capacity building in a range of Asia/Pacific countries, usually under the auspices of the International Telecommunication Union Development group (ITU-D) or via the APEC-Tel committee. Other nations have also been active in capacity building in a range of geographies under other organisations.

This work is vital. However, the question of how best to coordinate this activity across the globe is a vexed one since no single organisation has the reach and the technical and legal credibility to perform this task. It necessarily requires collaboration between a wide range of organizations for this to be achieved. The UN agency which is probably best placed to perform such a role may be the International Telecommunication Union (ITU) since it already performs extensive capacity building activity of its own through its ITU-D group. However, a broader scale of global collaboration in this space would require ITU-D's activities to be more effectively coordinated with the activities of a range of other global organisations such as ICANN and the Internet Society, as well as key regional groups such as APEC and the Council of Europe, together with appropriate private sector groups including the technical community that has been discussed above.

It is tempting to conclude from this brief discussion of the range of players which need to be involved, that some new entity needs to be established to be able to perform this coordination role effectively. However, Internet Australia believes that the practical difficulties of creating yet another group in this space mean that it is probably more sensible for the UN to find ways to coordinate the efforts of the existing players through existing frameworks. Whatever group or grouping of groups pursues this issue, a critical first step would be to embark upon a high level global audit of the

capabilities of national legal and enforcement frameworks and cyber detection and responsiveness capacities. This would provide the base information to inform where cyber capacity building efforts should be best focussed. This is a role which the UN Groups of Governmental Experts (UNGGE) could clearly progress in the short term.

We would be happy to elaborate further on ways to pursue this if DFAT wishes to discuss.

About Internet Australia

Internet Australia is the not-for-profit organisation representing all users of the Internet. Our mission – "Helping Shape Our Internet Future" – is to promote Internet developments for the benefit of the whole community, including business, educational, government and private Internet users. Our leaders and members are experts who hold significant roles in Internet-related organisations and enable us to provide education and high-level policy and technical information to Internet user groups, governments and regulatory authorities. We are the Australian chapter of the global Internet Society, where we contribute to the development of international Internet policy, governance, regulation and technical development for the global benefit.

Yours Sincerely

Dr Paul Brooks
Chair - Internet Australia
chair@internet.org.au