Asia Pacific Network Information Centre
APNIC Pty Ltd
ABN: 42 081 528 010

6 Cordelia Street
PO Box 3646
South Brisbane
QLD 4101 AUSTRALIA

URL www.apnic.net
Enquiries helpdesk@apnic.net
Accounts billing@apnic.net
Phone +61 7 3858 3100
Fax + 61 7 3858 3199

28/01/2020

To: Johanna Weaver

Special Adviser to Australia's Ambassador for Cyber Affairs and Representative to the UNGGE

From: Pablo Hinojosa

Strategic Engagement Director

Re: APNIC's response: Responsible state behaviour in cyberspace

Ref: Public consultation: Responsible state behaviour in cyberspace in the context of international security at the United Nations[1]

Dear Johanna,

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.[2] APNIC is offering the views expressed below, in our capacity as a regional Internet organisation, for any governmental or multilateral organization willing to engage with the technical community, in particular, Internet network operators and emergency response teams (CERTs or CSIRTs), to promote – as stated in the UNGGE objectives– an open, secure, stable, accessible and peaceful Internet.[3]

[1] "Public Consultation: Responsible State Behaviour in Cyberspace ..." *Department of Foreign Affairs and Trade*. 2 Dec. 2019. https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/public-consultation-responsible-state-behaviour-in-cyberspace-in-the-context-of-international-security-at-the-united-nation.aspx .
[2] Also noting: "IGF engagement in action: Cyber Norms" *NetThing*. 28 Oct. 2019. Video available here: https://youtu.be/bmq0eU2sEPk
[3] "A/70/174 - UNGGE Report, 2015." General Assembly, 70th session. *United Nations*. https://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/174.

Background

1. We live in a time where not only non-State actors commit cybercrimes, but also there is adverse cyber activity sponsored by States for espionage and/or military purposes. These actions may utilise cyberspace to affect sensitive components of the physical world, with consequences including jeopardizing human life.
2. Starting back in 1998 States began to discuss at the United Nations General Assembly First Committee developments in the field of ICT in the context of international security. In the intervening years, various multilateral processes to moderate cyberwar escalation have failed to gain traction or yield practical results. In spite of six different UN Groups of Governmental Experts (UNGGE)[4] mandated since 2004 to advance responsible State behaviour in cyberspace, and a new Open-Ended Working Group (OEWG)[5] to further develop this goal, the probability of States reaching meaningful agreements on cybersecurity appears to be very low.[6] [7]
3. There have been two reports by UNGGE, one in 2013[8] and a second one in 2015[9], where a small group of States have recommended a suite of voluntary, non-binding cybersecurity norms to apply during peacetime. While these reports support the notion that international law applies to State activities in cyberspace, the substance of those proposals is mainly political.
4. International cybersecurity discussions amongst States at the UN have been largely detached from technical considerations about the operation of networks. Furthermore, 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.
5. Without knowledge exchange and engagement between policy experts and network experts, the proposed cybernorms by the UN fail to recognize the practices that underpin the design, maintenance, security and operation of networks. For UN cybernorms to be useful, and to have any meaningful effect, it is essential to develop them in full consideration of detailed technical factors to determine whether

[4] "Group of Governmental Experts – UNODA." *United Nations*. https://www.un.org/disarmament/group-of-governmental-experts/.
[5] "Open-Ended Working Group – UNODA." *United Nations*. https://www.un.org/disarmament/open-ended-working-group/ .
[6] Korzak, Elaine (2017). "UNGGE on Cybersecurity: The End of an Era?" *The Diplomat*. 1 Aug. 2017. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ .
[7] Bowcott, Owen (2017). "Dispute along Cold War Lines Led to Collapse of UN Cyberwarfare Talks." *The Guardian*. 23 Aug. 2017. https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges.
[8] "A/68/98 - UNGGE Report, 2013." General Assembly, 68th session. *United Nations*. https://www.un.org/ga/search/viewm_doc.asp?symbol=A/68/98.
[9] "A/70/174 - UNGGE Report, 2015." General Assembly, 70th session. *United Nations*. https://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/174.

they can be feasible and implementable. Bridging the divide between the policy and technical communities, is an essential step in resolving the common disconnect between development of norms, and their effective implementation.[10]

6. There are two important groups within the technical community 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 CERTs.[11] 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.[12]
7. Recent developments and dialogues within the technical community have started to cautiously approach the international debates on cybersecurity norms.[13] Initiatives by the Global Commission on the Stability of Cyberspace (GCSC)[14], multistakeholder dialogues at UNIDIR[15] [16] [17], the Global Conferences on Cyberspace (GCSC)[18], and discussions at the IGF[19] are some examples of ongoing and emerging conversations. Governmental representatives at UNGGE and OEWG should not only actively engage in these conversations and use technical perspectives to inform their positions, but also take serious note of NOG[20] and CERT/CSIRT conferences and events[21].
8. Unfortunately, the measures that many States take for purposes of pervasive monitoring and widespread (often covert) surveillance often weaken Internet security. To dilute Internet security, whether knowingly or by consequence of other actions,

---

[10] Hinojosa, P., Aiken, K., Hurel, L. (2020) Putting the technical community back into cyber (policy). In: Tikk, E., Kerttunen, M. (eds) *Routledge Handbook of International Cybersecurity 1st Edition*. Forthcoming. Available from: https://www.routledge.com/Routledge-Handbook-of-International-Cybersecurity-1st-Edition/Tikk-Kerttunen/p/book/9781138489011.

[11] Hinojosa, P., Aiken, K., Hurel, L. (2020) Putting the technical community back into cyber (policy). In: Tikk, E., Kerttunen, M. (eds) *Routledge Handbook of International Cybersecurity 1st Edition*. Forthcoming. Available from: https://www.routledge.com/Routledge-Handbook-of-International-Cybersecurity-1st-Edition/Tikk-Kerttunen/p/book/9781138489011.

[12] Kolkman, Olaf. (2015) "Collaborative Security: An Approach to Tackling Internet Security Issues." *ISOC*. 12 Apr. 2015, www.internetsociety.org/collaborativesecurity/approach/ .

[13] Carr, Madeline. (2019) "Tech Community has a role to play..." *APNIC Blog*. 19 Dec. 2019, https://blog.apnic.net/2019/12/20/tech-community-has-role-to-play-in-improving-efficiency-of-cybernorms/ .

[14] "Global Commission on the Stability of Cyberspace." *GCSC*. https://cyberstability.org/ .

[15] "International Security and Cyber: UN Responses and Multi-Stakeholder Consultations." *UNIDIR*. www.unidir.org/events/international-security-and-cyber-un-responses-and-multi-stakeholder-consultations .

[16] "2019 Cyber Stability Conference." *UNIDIR*. www.unidir.org/events/2019-cyber-stability-conference .

[17] "Operationalizing Cyber Norms: Multi-Stakeholder Approaches to Responsible Vulnerabilities Disclosure." *UNIDIR*. www.unidir.org/events/operationalizing-cyber-norms-multi-stakeholder-approaches-responsible-vulnerabilities .

[18] "Global Conference on Cyber Space." *GFCE*. https://www.thegfce.com/about/gccs

[19] Hinojosa, P. (2019) "Bridging the policy and technical communities …" *APNIC Blog*. 25 Nov. 2019. https://blog.apnic.net/2019/11/25/bridging-the-policy-and-technical-communities-on-international-cybersecurity-discussions/.

[20] "Supporting Network Operator Groups." *APNIC*. www.apnic.net/community/support/network-operator-groups/ .

[21] "Security Cooperation." *APNIC*, www.apnic.net/community/security/security-cooperation/#CERTs .

can deeply threaten Internet operations, information security and personal privacy.[22] The fact that communications pass across networks owned, operated and maintained by private or public companies from different jurisdictions, must add pressure on States to ensure that the Internet is as free as possible from security loopholes and vulnerabilities. The operation of the Internet and the needs of its users are best served when the secure properties of connections across the Internet are preserved. This should be a guiding principle for responsible State behaviour in cyberspace, both domestically and internationally.[23] [24] [25]

9. Historically, Internet growth rates have been significantly higher than the rates at which a capable workforce becomes ready to maintain these networks, and there is no sign of a change in this condition. Because every security vulnerability originates in human behaviour (whether in human error, misunderstanding or oversight), resolving this skills shortage is a critical challenge in mitigating global cybersecurity risks. Therefore, States' commitment to build human cyber capacity at the technical and operational levels should be a top priority.
10. Lack of coordination in global cyber capacity building can produce unnecessary duplication of effort, either saturating communities or overlooking others. Having a clear map of organizations and initiatives is a prerequisite to avoiding such duplication, and to building partnerships for more effective and efficient outcomes. One key element of success is **a vendor and policy neutral approach** in all aspects of technical capacity building. While many alternatives are available provided by commercial vendors, genuine neutrality and technical objectivity are essential to building and maintaining trust in capacity building efforts and their outcomes.

Recommendations

APNIC recommends that governments:

1. Support efforts to open UN processes to offer more inclusive and diverse participation, in particular, for technical considerations to be brought into future cyber norm developments and their implementation, directly by practitioners.

---

[22] Recent amendments to the Australian Telecommunications Act to establish frameworks for industry assistance to law enforcement and intelligence agencies in relation to encryption technologies, has been controversial in this regard.
[23] "IAB and IESG Statement on Cryptographic Technology and the Internet" , RFC1984, *IETF*, August 1996, https://tools.ietf.org/html/rfc1984
[24] Farrell, S., and H. Tschofening (2014). "Pervasive Monitoring Is an Attack." RFC7258, *IETF*, May 2014, https://tools.ietf.org/html/rfc7258.
[25] "IAB Statement on Internet Confidentiality." *IAB*, 14 Nov. 2014, https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/ .

2. Promote active engagement from governmental representatives at the UN, in meetings such as AUSNOG (and other local and regional NOGs), AusCERT, PACSON, APCERT, FIRST, GFCE, GCCS, APNIC/APRICOT, APrIGF and IGF, with a view to integrating technical expertise and advice into UN discussions.
3. Strengthen collaboration with network operators and CERT/CSIRTs domestically to promote a trusted Internet environment. Responsible State behaviour to support an open, secure, stable, accessible and peaceful Internet starts at home.

APNIC further recommends that governments with more advanced cyber capabilities should fund and participate in cyber capacity building in countries that are their neighbours and trading partners, keeping the following principles in mind:

1. Addressing the growing demand for cyber capacity, particularly in less developed countries, must begin by understanding the local contexts in which content and delivery strategies can be meaningful and fit for purpose.
2. Template approaches can bring efficiencies but without care, may do more harm than good, as they are not tailored to the local needs.
3. Parallel to building individuals' knowledge and expertise, efforts to strengthen organizational capacity are also needed, to generate employment opportunities so that the trained professionals have opportunities to advance their careers locally rather than through migration.
4. Developing a full curriculum for continuous development, and generating opportunities to complete this curriculum, is important to prevent recipients from attending basic training repeatedly without progressing to more advanced levels.
5. Sponsoring local leaders, supporting train-the-trainers programs, encouraging local coordination and cultivating local partnerships are all important elements of successful cyber capacity efforts.
6. In addition, initiatives to support women's participation in industry and focused efforts on youth and earlier career development, are issues that merit global attention.
7. Collaborative approaches to develop educational material for both online and face-to-face delivery, are a great mechanism to align capacity building efforts. Local review mechanisms for curation of such materials will help to identify and promote best practices. Efforts to translate such educational content into local languages is a key element for adoption of best practices. Online training, especially for basic level trainings, is the most cost-effective and scalable way for delivery. It is also easier to do multilingual with online training for content localisation.

About:

APNIC is an open, member-based, not-for-profit organization, whose primary role is to distribute and manage Internet number resources (IP addresses and AS numbers) in 56 economies of the Asia Pacific region. As part of this service, APNIC is responsible for maintaining the public APNIC Whois Database[26] and managing reverse DNS zone-delegations[27]. APNIC also provides forums for Internet policy development[28], that are bottom-up and open to everyone. Furthermore, APNIC helps build technical skills[29] across the region, supports Internet infrastructure development, produces insightful research[30], and is an active participant in the multistakeholder model of Internet cooperation and governance. APNIC performs these activities as part of its commitment to a global, open, stable and secure Internet.

Acknowledgements:

While many staff members of APNIC contributed to this submission, we would like to extend our thanks to our friends Madeline Carr, Louise-Marie Hurel, Mika Kertunnen, Olaf Kolkman, Andrew Maurer, Elizabeth Oluoch and Rajnesh Singh for offering constructive feedback.

[26] See also: https://www.apnic.net/about-apnic/whois_search/about/
[27] See also: https://www.apnic.net/manage-ip/manage-resources/reverse-dns/
[28] See also: https://www.apnic.net/community/policy/
[29] See also: https://training.apnic.net/
[30] See also: http://labs.apnic.net/