SEOUL CONFERENCE ON CYBERSPACE 2013

ICT4Peace Special Session: Norms and CBMs - Moving towards a More Inclusive Agenda

ICT for peace foundation

Seoul Conference on Cyberspace 2013

ICT4Peace Special Session: Norms and CBMs - Moving towards a More Inclusive Agenda

17 October 2013, COEX Conference Center

Summary Report

On 17th October 2013, the ICT4Peace Foundation organized a special session on Norms and Confidence Building Measures (CBMs) in the margins of the 2013 Seoul Conference on Cyberspace.[1] Core speakers at the event, which was chaired by Amb. (ret.) Daniel Stauffacher, ICT4Peace, and moderated by Dr. Eneken Tikk-Ringas, Senior Fellow on Cyber Security, IISS, and Senior Advisor, ICT4Peace Foundation, included Ms. Christine Runnegar, Director of Public Policy at the Internet Society (ISOC), Mr. Matt Thomlinson, General Manager for Trustworthy Computing at Microsoft, and Zahid Jamil, Director at the Developing Countries' Centre for Cyber Crime Law. Ms. Camino Kavanagh, PhD Candidate, Kings College London and Senior Fellow, NYU was Rapporteur of the Session. Each speaker provided insights into some of the complex international security-related issues surrounding cyberspace and the use of ICTs, and their views on how the current dialogue on norms and confidence building measures (CBMs) can be bolstered. The approximately 45 participants included senior representatives from governments, industry, civil society and research institutions and academia, who actively participated in the ensuing discussion on progress made within on-going norms and CBM processes. ICT4Peace's Daniel Stauffacher was invited to report on the results of the session to the plenary of the Conference (see his statement attached in Annex 1).

There was broad consensus among workshop participants that current norms and CBM processes need to be underpinned by the principles of shared responsibility, responsible behaviour, inclusion, collaboration and transparency. In this regard, collectively sharing the responsibility of managing international cyber security risks among all stakeholders can help build trust across countries and regions. A more inclusive agenda which draws on expertise from across sectors and across regions, can foster greater collaboration and transparency, affording more legitimacy to on-going processes; and greater transparency can help identify gaps, ensuring more targeted and common responses to challenges and risks that emerge. At the same time however, these principles – and particularly the principle of responsible state behaviour - require much more discussion, not least because of opposing state views on how they are currently guiding state practice.

Presentations by Ms. Runnegar and Mr. Jamil spurred discussions on the importance of:

- Finding more compelling ways to level the playing field, for example, by providing targeted capacity building, linked not only to the needs and interests of developed states, but based on an informed dialogue with developing countries around gaps,

[1] For more information on the Conference and its underpinnings see: http://www.seoulcyber2013.kr/en/main/main.do

needs and interests. The latter can help trigger a move away from the 'us' and 'them' approach to cybersecurity (vis-à-vis cyber and ICT capabilities) that has dogged discussions on the topic to date, while affording more legitimacy to on-going processes aimed at cybersecurity problem solving. Emerging economies in particular can play an important role in supporting capacity building efforts. Increased effort should also be made to tie capacity building efforts in this field to development policy and practice.[2]

- Providing an effective means for deepening understanding and communicating ideas and opinions, while also respecting the language, culture, education, ability, location, and other circumstances, of key partners. This is a much deeper task than understanding another country's or another stakeholders' narrative,' and requires a deeper understanding of the political economy and different pressures at play in a given setting.

- Ensuring that a broader spectrum of relevant government institutions beyond core security services (and particularly those in leadership/ decision-making positions), participate in regional and international meetings on cyber security (e.g. on protection of critical infrastructure); and that capacity building efforts include a focus on integration of effort across institutions at the national level.

- Ensuring an effective channel for contributions and advice from a broader spectrum of actors for example, to the GGE, which is an inter-governmental process, so as to ensure that decisions regarding international cyber security are not skewed in favour of those groups with the most resources (time, money, political influence, etc.).

- Finding the most effective means to share responsibility and build in accountability to decisions made with regard to international cybersecurity.

- Determining the most effective way to represent the "public interest" not least because of the role citizens play in upholding norms.

- Garnering lessons from open source culture and practices.

Building on Mr. Thomlinson's presentation, participants also discussed the manner in which the current dialogue around norms is hampered by the fact that most efforts still concentrate on low-probability high-end threats such as the military uses of cyber capabilities by states during armed conflict. While there is no doubt that the latter requires significant attention, not least in relation to how international law and the UN Charter is applicable in such circumstances,[3] participants also stressed the importance of focusing efforts on seeking a common framework to respond to the kinds of threats (e.g. cybercrime, damage to critical infrastructure, IP theft, exploitation of government systems, or criminal attacks against citizens) that affect citizens, governments and businesses on a daily basis. In this regard, Mr. Thomlinson tabled five principles as an example of what might underpin diplomatic efforts aimed at agreeing on a set

[2] See for example, Art. 33 of the UN GGE Report (A/68/98) - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security - which recognized that "progress in securing the use of ICTs, including through capacity-building, would also contribute to the achievement of Millennium Development Goal 8, to "develop a global partnership for development".

[3] The question of whether international law and the UN Charter are applicable or not to cyberspace was resolved in the UN GGE Report (A/68/98), which noted in Art. 19 that [i]International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." Meanwhile, Art. 20 noted that "[s]tate sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." (A/68/98). An important next step will include moving from ***if*** to ***how*** these core instruments and principles apply. See Footnote 4 below for an explanation of the GGE process .

of common norms to respond to these kinds of challenges.[4] The five principles include harmonization of laws and standards; risk reduction; transparency; collaboration; and proportionality.

These are evidently issues that cannot be approached by one single government, group of governments, private company or organization. Rather, all stakeholders have a shared interest in ensuring that our societies continue reaping the enormous benefits of ICTs, while also ensuring effective responses to challenges that might emerge in cyberspace and through the malicious use of ICTs. In this regard, the outcome of the recent UN GGE report (A/68/98)[5] was an important milestone on several fronts, including its recognition of the importance of civil society and industry expertise in informing discussions on how best to cooperate in implementing norms and principles of responsible behaviour in cyberspace;[6] and the role of research institutions and universities in supporting capacity building efforts "through further analysis and study on matters related to ICT security."[7]

In this regard, participants noted that industry, civil society and researchers could establish a platform, pulling together and amplifying their views as a means to help governments improve their own understanding and policy-making processes with regard to international cybersecurity. Such a process should draw on a wide range of geographic perspectives, especially those regions that have been less engaged in the cybersecurity debate to date. At the same time, it will be important to bear in mind the trade-offs between efficiency and the legitimacy of a participative process, ensuring that such a process is sufficiently robust and resourced to remain effective, and that it is strategic in how it makes itself heard above all the existing noise. As a first step in this direction, ICT4Peace has offered to serve as an initial focal point for establishing this initiative into a scalable and sustainable process. More details on the initiative will be communicated in the coming months.

Camino Kavanagh, Seoul, 18 October 2013

[4] In its most recent White Paper, Microsoft noted that five core principles for cyber security norms could include harmonization of laws and standards; risk reduction; transparency; collaboration; and proportionality. In particular, the paper centres these around some of the core [below-the-threshold] international cybersecurity themes currently being discussed in international fora, including: avoiding conflict; managing threats and vulnerabilities; building trust and transparency; sharing threat and vulnerability information and coordination among states; and cybersecurity capacity building. Microsoft (2013), White Paper: Five Principles for Cybersecurity. See: http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Five_Principles_Norms.pdf

[5] Bearing in mind that international cooperation is essential to reducing risk and enhancing security against the malicious use of ICTS, in 2010 the UN General Assembly requested the Secretary-General, with the assistance of a group of governmental experts, to continue to study possible cooperative measures to address existing and potential [ICT-related] threats (resolution 66/24), and submit a report to the sixty-eighth session of the Assembly. The report (A/68/98) builds upon the 2010 report (A/65/201).

[6] Art.s 12, 24, 25 and 28 of A/68/98

[7] Art. 32 of A/68/98

ANNEX 1

Seoul Conference on Cyberspace 2013

Statement by Daniel Stauffacher, President, ICT4Peace Foundation to the Seoul Conference

Excellencies, Ladies and Gentleman,

Yesterday, A number of important interested stakeholders from industry, technical community, civil society, academia and government met to discuss recent progress in the development of cyber norms and confidence building measures.

We agreed that norms and CBM processes need to be underpinned by the principles of shared responsibility, responsible behaviour, inclusion, collaboration and transparency.

We welcomed the fact that UN GGE Report (A/68/98) recognised the importance of drawing on civil society and industry expertise and agreed that industry, civil society and academia should work together to establish a platform to pull together and amplify their views.

We agreed on the importance of ensuring that this process draws on a wide range of geographic perspectives, especially those regions that have been less engaged in the debate to date.

We called on all governments to take advantage of the insights that industry, civil society and academia can provide in order to improve their own policy-making processes.

We noted that ICT4Peace will provide an initial focal point for establishing how this initiative can be developed into a scalable and sustainable process.

Seoul, 18 October 2013

ICT4Peace Foundation
www.ict4peace.org

ICT4Peace was launched as a result of the World Summit on the Information Society in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between peoples, communities and stakeholders involved in conflict prevention, mediation and peace building through better understanding of and enhanced application of Information Communications Technology (ICT). In the field of Cyber Security ICT4Peace is interested in following, supporting and leading bilateral and multilateral diplomatic, legal and policy efforts

to achieve a secure, prosperous and open cyberspace.

The following ICT4 Peace publications on cybersecurity and resilience can be found at: http://ict4peace.org/?p=1076

- Getting down to business: Realistic goals for the promotion of peace in cyber-space
- (2011)
- ICT4Peace brief on upcoming Government Expert consultations on Cybersecurity
- (GGE) at the UN in New York (2012)
- An overview of global and regional processes, agendas and instruments (2013)
- Confidence Building Measures and Cybersecurity (2013)
- The Reach of Soft Power in Responding to International Cybersecurity Challenges (2013)

Follow ICT4Peace on Twitter here - http://www.twitter.com/ict4peace
Follow ICT4Peace on Facebook here - http://facebook.com/ict4peace