International Workshop on Information and Cyber Security

Towards a Peaceful, Secure, Open and Cooperative Cyberspace

5-6 June, Beijing, China

SUMMARY REPORT[1]

[1] The views contained in this report do not necessarily reflect those of the UNRCPD.

Executive Summary

In the Internet's 20 year history, international cyber threats are rapidly emerging and complex, touching on many facets of everyday life. Building on the UN Group of Governmental Experts' (GGE)[2] landmark international consensus of June 2013 (A/68/98*), this multi-stakeholder workshop gathered 74 senior officials from 25 member states at the policy and technical levels and included representatives from academia, private sector, civil society and UN organisations to discuss a range of cyber security issues. The discussion was interactive, wide ranging, and balanced, debating possible responses to various cyber threats, and helping to build trust at a time when international relations on cyber issues face increasing challenges.

Delegates cited the 2013 GGE report as proof that compromise on cyber security issues is indeed possible, and highlighted the current window of opportunity to enhance national, regional and international measures to establish a peaceful, secure, open and cooperative cyber space. Representatives also pointed to the GGE report and reaffirmed that international law is applicable to the use of ICTs by states, but discussed how this might be done to meet the needs of states. 'The application of norms derived from existing international law relevant to the use of ICTs by States is an essential measure to reduce risks to international peace, security and stability. Common understanding on how such norms shall apply to State behaviour and the use of ICTs by States requires further study. Given the unique attributes of ICTs, additional norms could be developed over time'[3]. Proposals included elaborating the practical application of existing international humanitarian law, and formulation of new norms or rules for state behaviour. Some pointed to the International Code of Conduct for Information Security proposed by SCO member states in 2011 (A/66/359) as a helpful effort to facilitate international discussion on norms and rules, and welcomed suggestions on how to improve it.

Delegates also floated proposals such as: (1) at a minimum, 'red lines' of state behaviour in cyber space should be adopted as has been done in other areas, (2) humanitarian 'safe zones' analogous to Geneva Convention provisions could be considered; and deliberated on multiple facets of some proposals such as: the applicability of existing international laws signifying that the principle of State Sovereignty, non-interference in other countries' internal affairs and prohibition of use of force anchored in UN Charter apply to the cyber space. Some delegates maintained that the Law of Armed Conflict derived its legitimacy in cyber space from the applicability of existing international laws. Others warned that given the unique attributes of cyber space, rushing to such a conclusion without prudent discussion could run counter to the common aspiration of preserving the peaceful nature of cyber space.

There was wide support for increased confidence-building measures (CBMs), including transparency, cooperation and stability variants, especially at the regional and policy levels. The workshop itself acted as a CBM, as some pointed out, bringing to the fore various threat perceptions, policy responses, and response implementation challenges, including speed, user anonymity, coordination amongst actors with disparate technical understanding, human resources capacity, intangible return on investment and 'proliferation of international meetings'. Some noted that existing mutual legal assistance treaties on cyber crime could be used as a *de facto* authorisation to increase CERT-CERT information sharing and enhance technical levels of trust.

Delegates agreed that since CBMs rely in part on state capacity, CBMs must be accompanied by capacity-building activities to assist states, including : (1) help in formulating national strategies/legislation, (2) building detection/response capacities at policy and technical levels, (3) enhancing horizontal/vertical coordination between and within agencies, and (4) increased development aid to bridge the digital divide. Some delegates also cautioned that increased attention by policy actors to inter-CERT coordination and new bureaucratic processes had in some

[2] 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (GGE).
[3] Quote from paragraph 16 of the 2013 GGE report.

cases unintentionally hindered timely information sharing and cyber incident resolution, and attention should be paid to avoid such a situation in the future.

In an era of hyper-connectivity, many emphasised cyber crime's threat to societies and discussed the Budapest Convention's regional appropriateness and effectiveness as a response measure. Threats to individual privacy were highlighted, with delegates proposing private sector, regional and UN responses. The risks of 'free flow of information' were deliberated (including what some saw as spreading of misinformation, fomenting of social unrest or infringement on culturally-specific rights), along with concerns that restricting information flow could hinder economic and social development, it was noted by one delegate that the realization of freedom also relied on 'secure flow of information'.

Internet governance was discussed, including the future mix of state, private sector and civil society influence over the use and evolution of the Internet. Views were expressed on various states' roles in regulating internet content and governance structures, with delegates concurring that state sovereignty covers internet infrastructure and public policy within jurisdictions. Delegates agreed on the need to preserve the Internet's value-generating creativity, ingenuity and reliable interoperability, and that multi-stakeholder influence over internet governance is essential to achieving this. There were several calls to extend the mandate and funding of the Internet Governance Forum (the UN-mandated multi-stakeholder forum for policy dialogue on internet governance), and for a clear division of labour between discussion fora.

Overall, the workshop: highlighted several areas of convergence, including the need to tackle cyber crime via international cooperation and law; identified several common cyber response challenges facing states; witnessed increased calls for trust-building between all stakeholders including states; recognised the importance of multi-stakeholder internet governance for the Internet's future health; and generated proposals for international norms of state behaviour. Participant feedback was overwhelmingly positive, with many commenting on how the workshop achieved relevant, frank and balanced discussions, adding that it was a key event to help build trust on critical issues, and that it came at a crucial moment in international discussions. Delegates all expressed hope for further constructive dialogue and galvanised consensus during the next GGE session in 2014 and beyond.

Contents

Introduction

The United Nations Office for Disarmament Affairs (UNODA), through its Regional Centre for Peace and Disarmament in Asia and the Pacific (UNRCPD), the Ministry of Foreign Affairs of the People's Republic of China, and China Arms Control and Disarmament Association, jointly organized an 'International Workshop on Information and Cyber Security: Towards a Peaceful, Secure, Open and Cooperative Cyberspace', in Beijing, China, on 5-6 June 2014. The workshop built on the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of June 2013 (A/68/98*). Senior officials involved in national policy coordination on cyber security issues discussed the topics: Cyberspace Policies and Emerging Challenges, Formulation of International Rules and Norms in Cyberspace, The Role of the United Nations in promoting Dialogue on Cyber Security, Interaction and Cooperation between National Level Actors, and Regional Dialogue, Cooperation and Capacity Building.

Mr. Li Baodong, Vice Foreign Minister of China, attended the opening session of the workshop. In his keynote speech, he expounded on four principles to be upheld in cyberspace, namely, peace, sovereignty, co-governance and universal benefit.

He reiterated China's position against the militarization of, and an arms race in, the cyberspace. He maintained that the principle of state sovereignty, is applicable to the cyberspace, including at least the following factors: states own jurisdiction over the ICT infrastructure and activities within their territories; national governments are entitled to making public policies for the Internet based on their national conditions; no country should use the Internet to interfere in other countries' internal affairs or undermine other countries' interests. He also called for efforts to build a global Internet governance system that is fair and equitable, in line with the principles of multilateralism, democracy and transparency, as well as increased assistance to developing countries aimed at bridging the 'digital divide'.

Advocating a peaceful, secure, open and cooperative cyber space, Mr. Li emphasized the importance of dialogue and cooperation, universally accepted international norms on state behaviour, and the equal participation of all parties in the discussion of cyber issues facing the international community.

A message from Ms. Angela Kane, High Representative for Disarmament Affairs was delivered by Mr. Jarmo Sareva, Deputy Secretary-General of the Conference on Disarmament and Director, Office for Disarmament Affairs, Geneva Branch.

In her message, Ms. Kane recognized both the enormous benefits as well as the increasing risks associated with ICT on a daily and global basis. She reaffirmed that solutions for ICT security need to be anchored within the existing framework of international law and understandings that govern State relations. For that reason, she expressed her support for the process as it was carried out, highlighting the cooperation between UNRCPD and the Chinese government. She argued for the importance of dialogue in reaching solutions that are compatible internationally, at the bilateral, regional and multilateral levels, as well as institutional dialogue with broad participation under the auspices of the United Nations.

She concluded by reaffirming the importance of confidence-building measures in cyber-security, as a means of reducing the risk of conflict, misperception and miscalculation by promoting trust and increasing predictability.

Session I: Cyberspace Policies and Emerging Challenges

Sri Lanka CERT/CC
Operations Manager & Principal Information Security Engineer

The representative from the Sri Lankan state-owned CERT Coordination Centre (CERT|CC) outlined Sri Lanka's cyber situation, response measures, current challenges and proposals to overcome those challenges.

With internet reaching 20% of Sri Lanka's population, cyber crime is rising and potential strikes on critical national information infrastructure are the main cyber threats facing Sri Lanka. In response, Sri Lanka: (1) set up Sri Lanka CERT|CC as the national centre for cyber security, (2) adopted a High Level Information Security Policy and e-Government Policy, (3) enacted the Computer Crimes Act in 2008 for the prosecution of computer crimes, (4) created a Computer Crimes Division within the Sri Lanka police, including a digital forensic lab, and (5) created ongoing awareness-raising activities for the general public through the Sri Lanka CERT/CC.

Implementation challenges include user diversity, network complexity, hardware and personnel shortfalls (e.g. no national level security operations centre), difficulty in convincing that proper security solutions are a good investment , and limited cooperation between key actors inside and outside the country (e.g. between law enforcement and internet service providers/foreign webmail or social networking platforms). Differing policies and cultural attitudes towards freedom of expression make the classification of 'criminal speech' different in every country, thus harder to prosecute.

To overcome these challenges it was proposed to formulate contextually-adapted national strategies (aligned with international standards), continue to raise public awareness, increase local and international coordination, and request the sharing of resources from more developed countries (*e.g.* intelligence information, resources, technology and expertise).

New Zealand
Policy Officer, International Security and Disarmament Division, Ministry of Foreign Affairs and Trade

The country's primary cyber threats, responses and response implementation challenges were outlined. Whilst the country faces a range of cyber risks (cyber bullying, spam, crime, theft, attacks on critical information providers, state-sponsored espionage, and military use of cyber tools), some of the most common are disruption of service and cyber crime-related attacks.

In response, the country's 2011 strategy aims to: (1) raise awareness and online security, (2) protect government systems and information, and (3) plan and execute incident response. In 2012, the National Cyber Policy Office (NCPO) was established within the Prime Minister's Office to coordinate cyber security responses across government agencies. Alongside new legislation (amending the Government Communications Security Bureau Act, and the Telecommunications Interception Capabilities and Security Act 2013), New Zealand has conducted outreach to engage critically important stakeholders (including the private sector), raised public awareness on cyber risks and shared best practices with international partners.

Looking forward, NPCO is also refreshing New Zealand's cyber security strategy (for end 2014) and intensifying international engagement. Future challenges include: keeping up with cyber threats' pace of change, horizontal policy coordination between agencies, vertical functional coordination within sectors, and resourcing participation in proliferating international cyber meetings.

Japan
Ambassador in charge of UN Affairs and Cyber Policy, Foreign Policy Bureau

International challenges and responses were outlined, and emphasis was placed on the importance of maintaining free flow of information in cyberspace. Four key challenges are: (1) all-pervasiveness of cyber space in business and daily life, (2) user diversity (including economic, political and criminal actors), (3) anonymity, difficulty of tracing actions, potential for misattribution and escalating mistrust, and (4) speed of change and inability of policy to keep pace.

Proposed solutions included: (1) application of existing international law to cyber space, (2) confidence-building across diverse actors (including states, private corporations and CERTs), and (3) building developing countries' capacity to mitigate emerging cyber vulnerabilities. Through capacity building, the country aims to support developing countries' sustainable growth, social stability, and public-private partnerships, as well as enhancing global security. Whilst the near-term priority is to assist ASEAN countries, longer term Japan looks forward to expanding assistance to other countries in Asia-Pacific and Africa.

Free flow of information is vital for a country's social, but also economic development. Japan supports unrestricted content and interoperability online, and a continuation of a non-state-led, multi-stakeholder approach which gave rise to the Internet's value.

Pakistan
Director of Cyber Security, Ministry of Defence

Key national threats were outlined, such as organised cyber crime, cultural infringements, social destabilisation, attacks on national critical infrastructure, and proposed responses were put forward. Today's hyper-connectivity and extreme mobility have exposed mankind to new vulnerabilities and insecurity.

With electronic/cyber crimes as the country's main cyber security issue, they adopted an Electronic Crime Ordinance in March 2014. The Ordinance addresses, *inter alia*, unauthorised calls and attacks against individuals, organisations and the government. A proposal was put forward for an international cyber court (akin to the International Criminal Court) to establish a process which could convict international cyber criminals.

It was noted that in some contexts freedom to publish online, where through one click anyone may reach millions, threatened to harm culturally-specific liberties and possibly destabilise societies. It was proposed that a degree of restriction is needed on freedom of expression, to regulate each individual's immense power of online publication and prevent harm to other cultures and societies.

The emerging threat of criminal cyber attacks against any nation's critical infrastructure also demanded formal or informal international cooperation among CERTs. An international treaty is needed to guarantee rapid information sharing in case of cyber attacks.

Discussion

During ensuing discussion, other state representatives outlined their cyber space goals and policies, discussed the principles of online content flow and related international frameworks, CERT-CERT information sharing, and the format for productive future discussion.

One explained China's national cyber challenges and efforts to enhance both national and global cyber security, including balancing security and development in cyber space. China pursues the role of a strong cyber state and recently established a national leading group on cyber security and informatization, responsible for strategic guidance and national coordination. An Office for Cyber Affairs was also formed within the Ministry of Foreign Affairs.

Another delegate explained Malaysia's experience of increased recent cyber attacks, cyber space goals (preserving national identity online, digital border protection, and public awareness and appreciation of ICT), and cyber security oversight/direction structure under its National Security Council. The representative described policy components, whose implementation is supervised by task forces, including: (1) critical information infrastructure protection, (2) content and cyber crime management, (3) cyber crisis management, (4) legislation, (5) capacity building, and (6) compliance/enforcement. Its cyber crisis management committee and plan has conducted annual exercises since

2008, and recognises that private sector stakeholders are key to addressing cyber threats. The national vulnerability assessment programmes were outlined as well as efforts to encourage international information security standards.

South Africa's challenges were described, including dependence on non-domestic ICT and keeping pace with technological change. Responses included the formation of an interdepartmental cyber security response committee, ongoing policy and strategy formulation (on all areas including cyber crime and protecting critical information infrastructure), capacity building (with private sector and academia) and international cooperation.

Participants discussed the 'free flow of information'. One argued that in a big data era, states should legislate and regulate content to ensure a 'free and secure flow of information', which is exemplified by many states' commitment to fighting against child pornography. Another agreed on the importance of secure information flow (especially against malware and phishing), but that the social and economic effects of restricting individual expression in cyber space crossed borders. One participant called for non-European states to join the Budapest Convention as a fast-track and well-written international agreement for ensuring secure information flow without policing 'thought crimes', while some were reluctant because they had not been involved in negotiating the instrument. Another individual mentioned that South Africa had signed the Budapest Convention but had not yet ratified it as South Africa was aligning its national legislation under a regional African Union convention against cyber crime. Several delegates noted that in practice, parties to the Budapest Convention rarely share information.

Several delegates emphasised the value of rapid CERT-CERT information sharing, and called on countries with more advanced CERTs to provide timely notice to less advanced CERTs – at least of threats identified, if not solutions. Given the speed of cyber attacks, the need for rapid information sharing about threats was repeatedly emphasised. Another delegate cited APCERT covering China, Japan and the Republic of Korea as an example of excellent international CERT-CERT cooperation. He also asserted a need for greater vertical cooperation between governments and CERTs (which may be publicly funded but legally private).

Another participant questioned how international meetings should be structured for maximal productivity, balancing participation across various stakeholder groups and increased specialisation into subareas (e.g. separating military, crime and secure information flow issues).

Session II: Formulation of International Rules and Norms in Cyberspace

China
Coordinator for Cyber Affairs, Ministry of Foreign Affairs

The representative outlined the country's position on formulation of norms and rules, internet governance and the GGE.

The speaker explained China's strong support for the formulation of international rules and norms to govern states' behaviour in cyber space, and drew attention to a draft International Code of Conduct for Information Security proposed by China and other SCO member countries in 2011, emphasizing that China regards this as an open document, and welcomes other states' views and proposals on it.

The country supports a multilateral, transparent and democratic model of internet governance, specifically: multilateral supervision of ICANN and giving the Governmental Advisory Committee (GAC) voting rights over ICANN's decisions, transparency over root zone files with ISSAC filing regular accountability reports, and an extension to the democratic Internet Governance Forum's funding, mandate and role in internet governance. They are not against a multi-stakeholder internet governance model, and stressed that the role of governments should not be marginalised in internet governance.

The speaker welcomed the 2013 GGE report as a balanced compromise between states. Calling for a holistic reading of the 2013 report, the envoy expressed China's support for further study of applying existing standards to cyber space (including principles of non-interference and peaceful conflict resolution), as well as new standards to supplement existing international laws. The representative called for a continuation of the balanced approach of 2013 in forthcoming GGE discussions. The speaker expressed strong concern over the practice of double standards on cyber related issues.

Germany
International Cyber Policy Coordinator, Federal Foreign Office

Speaking in a personal capacity, the representative suggested ways forward on GGE-related issues and on internet governance.

The UN-GGE 2013 report constituted a great achievement as it had, for the first time, brought general consensus on state responsibility, on applicability of international law and on confidence building in cyberspace. However, open questions remain, e.g. on the concept of sovereign boundaries in cyber space and on when cyber attacks would be counted as armed attacks under international law; the term 'cyber war' should therefore be used with caution. The representative suggested developing norms for state behavior below the threshold of armed conflict, placing limits on state cyber espionage and protecting privacy/intellectual property. One should also explore how to delineate humanitarian safe zones in cyber space.

On internet governance, the speaker underlined that a particular government's oversight over ICANN/IANA had nothing to do with capabilities for mass surveillance, although public debate often mixed these technically unconnected issues. The delegate acknowledged impressive success of the multi-stakeholder approach to regulate the use and evolution of the Internet. He doubted that a UN body could handle these tasks more efficiently or democratically. Cautious reform of ICANN was the right approach. However, the UN would remain the main forum for debating digitalization; the IGF's mandate should be continued.

Internet Corporation For Assigned Names and Numbers (ICANN)
Vice President and Managing Director

ICANN's representative explained why the Internet had flourished historically, and put forward a list of governance models would promote its continued flourishing in the future.

Conceptualising the Internet as a 'network of networks', he explained that online communication relies on interoperability between networks. The delegate detailed ICANN's role of ensuring such interoperability by assigning unique identifiers to users, and emphasised that during its 16 years such universal technical standards had been arrived at and preserved through ICANN's multi-stakeholder consultations, with key input from private sector actors. States also exercised guidance over ICANN's actions via the advisory GAC committee of 133 states. An example was given in which the GAC committee effectively used its channel to protect sovereign geographic names in the creation of new generic top-level domain names in a consultative process.

Looking forward, the speaker recognised that governments have a key role in averting cyber warfare and fighting cyber crimes, but argued that any increased state involvement in internet governance should avoid endangering the harmonised internet standards in place today. The delegate called for a continued and expanded multi-stakeholder process to ensure internet industries' future health. Welcoming the general principles of NETmundial as governance cornerstones, it was emphasised that future internet governance should take a more inclusive perspective and incorporate developing countries' voices, as well as ensuring that states were not marginalised in governance decisions. ICANN's initiatives to engage a broader representation of states, publics and other stakeholders via regional consultations were outlined.

Discussion

Discussion focused on privacy/surveillance, sovereignty and warfare in cyber space.

Discussants pointed out that the free flow of information does not make mass surveillance inevitable. One argued that unlike control over information infrastructure, a state's supervision of the Internet's 'logical' layer (i.e. the assignment of names and numbers to users) is unrelated to surveillance advantages. One asserted that the term 'mass surveillance' mischaracterises the activities of certain national intelligence agencies, which actually conduct targeted searches of user data for signs of terrorist activity or foreign espionage. Another noted that all states engage in some kind of cyber espionage, arguing the challenge lay in ensuring such activities do not destabilise state relations. One suggested developing rules of state behaviour relating to mass surveillance over humanity within the framework of the GGE.

Acknowledging the difficulties of interpreting the concept of sovereignty in cyber space, some delegates concurred that sovereign jurisdiction at least entailed the right to make public policy governing the Internet, and control over internet infrastructure within national jurisdictions. However, it was questioned whether sovereignty applied to information stored/flowing within national networks, noting the possibility that such sovereignty might be used to limit free access to information. Another argued that a well-regulated internet would not inevitably impede freedom of expression, and that some countries felt the need to prevent the spread of misinformation by other actors amongst their citizens .

Some urged disciplined use of the term 'cyber warfare', and questioned whether armed attacks existed in cyberspace, questioning whether any humans had yet been directly harmed, highlighting that militaries had long sabotaged enemy telecommunications as part of warfare. Others argued that societies' vulnerability to cyber attacks had reached historically unprecedented levels, and that recent trends (including use of offensive cyber weapons) presented a limited window of opportunity to enhance international security via cyber weapon control and conflict prevention. Some hoped that discussing the cyber conflict prevention as a matter of urgency could lead to international norms or 'red lines' of state behaviour in cyber space.

Session III: The Role of the United Nations in Promoting Dialogue on Cyber Security

UNIDIR
Programme Lead, Emerging Security Threats Programme

Speaking in a personal capacity, the UNIDIR representative called for developing rules of responsible state behaviour in cyber space to ensure cyber stability, and outlined how the UN might help. The delegate acknowledged that for many emerging states, their main interest in cyber space is currently socio-economic.

Eschewing the term 'cyber security', the participant instead suggested focusing on 'cyber stability' to prevent conflict contagion and escalation between the highly-related kinetic and cyber domains. The delegate noted that interstate agreement on common values might be too optimistic in the near term, calling instead for focus on formulating norms of state behaviour in cyber space to build confidence and predictability into interstate relations.

The participant noted that the UN faces unusual difficulties addressing or coordinating cyber security issues, as policy making is occurring simultaneously at national, regional and international levels. The participant called for: (1) segmentation of cyber security issues across UN discussion fora, (2) capacity building to facilitate common understandings of expectations regarding responsible state cyber behaviour, (3) the creation of a high-level UN position or role, rather than a new institution, to set the UN's direction on cyber issues and coordinate across existing dialogues. The speaker noted that the Internet's socio-economic benefits rely on cyber stability, and hoped for rapid progress towards predictability and confidence.

UNODC

Director of Division for Treaty Affairs

The UNODC representative outlined crime challenges in cyber space, and UN response roles such as problem analysis and facilitating dialogue.

The delegate noted that the Internet can be used for good or ill, with victimisation rates often higher for online than conventional crimes – and higher in developing than developed countries. To respond the UN should adopt a multidisciplinary approach encompassing security, development, crime, justice, economic, social and human rights perspectives from across the UN system.

Several UN roles were illustrated, including problem analysis (e.g. the comprehensive study on cyber crime mandated by General Assembly Resolution 65/230) and facilitating both interstate and intrastate dialogue amongst relevant stakeholder groups, including the recent GGE process, the post-2015 development discussion of the Open Working Group on Sustainable Development Goals and the World Summit on the Information Society. UNODC's progress in leveraging existing anti-crime conventions to facilitate dialogue on online drug trafficking, online child protection and cyber crime were described. The delegate emphasised the opportunity arising from the UN's multi-forum discourse, arguing that ignoring or isolating key cyber issues would hinder humanity's enjoyment of the Internet.

International Institute for Strategic Studies (IISS)
Director of Transnational Threats and Political Risk

The delegate contextualised cyber space issues, and suggested the UN play contrasting roles on issues of internet governance and interstate cyber conflict. The speaker noted that dependence on ICT meant humanity had to continue trying to find ways of managing and controlling the rapidly evolving cyber space environment.

On internet governance, the delegate suggested the ITU play a narrow technical role focused on extending the Internet's reach, rather than trying to displace existing governance arrangements (e.g. ICANN and IETF) – not least because existing arrangements have been relatively effective so far. The delegate acknowledged that existing arrangements favoured developed countries, but noted that mistrust between states made more intrusive UN involvement in internet governance politically challenging, as illustrated by the 2012 WCIT conference, when the western media stirred suspicions that it could lead to the ITU regulating the Internet.

On interstate cyber conflict, the delegate advocated a risk mitigation approach. Noting increased state appetite for offensive cyber capacities, the speaker argued that practical challenges would render agreements to control cyber weapons unverifiable and unenforceable (as with the Biological Weapons Convention). Instead, measures such as norms prohibiting cyber attacks on humanitarian or critical infrastructure safe zones could mitigate risks of conflict escalation. The representative spoke optimistically about the 2013 GGE compromise consensus. Outstanding challenges identified within the GGE process included: (1) the contentious issue of whether the Law of Armed Conflict can meaningfully apply within cyber space and (2) that normative behaviours are most likely to arise from bilateral agreements. It was suggested that the UN could help spread norms reached bilaterally throughout the international community.

International Telecommunications Union (ITU)
Cybersecurity Coordinator

The ITU representative argued the UN could help build a shared understanding of key concepts and terminology amongst stakeholders as a precursor to constructive dialogue. The speaker highlighted emerging risks in cyber space, including to critical infrastructure and to humans. Examples of cyber crime hacking software were also given. The delegate affirmed the UN's role as key facilitator of dialogue on addressing cyber threats and outlined various

ongoing discussions. It was argued that lack of shared understanding, especially on technical issues, hindered political trust and concerted action within and between states.

The speaker proposed that the UN could also play a capacity-building role by fostering shared understanding within states (horizontally between agencies and vertically between policy and technical levels) regarding basic technical realities of cyber space. This bottom-up approach would also involve developing national strategies, policies and response capacities, forming the foundation for states to participate coherently and purposefully in international dialogues. He also outlined the UN Secretariat's own seven basic principles for coherent direction when addressing cyber issues.

China Institute of Contemporary International Relations
Vice President and Research Professor

The representative highlighted the UN's distinguishing features in the contemporary setting and shared his outlook on what can the UN deliver in the future for cyber security.

The speaker argued the UN is currently unique in its authority, arising from state mandates and UN performance over the last 70 years, multilateralism, and its guiding principles of promoting equality, which should extend to the cyber realm.

The speaker made several recommendations for the UN to promote dialogue on cyber security: (1) exploit existing mechanisms to address cyber security, including the GGE, (2) expand the operational and technological capacity of UN on cyber security, (3) further discuss the role of the UN in addressing cyber security, (4) monitor the implementation of policies adopted in past conferences, and (5) incorporate more technical specialists in the conversation, learning from past UN experience in counter-terrorism and peacekeeping.

Discussion

Discussion covered the UN role as a discussion forum, merits and limitations of existing UN processes and extra-UN discussion fora.

Recognising the UN as a uniquely multilateral organization, delegates agreed that the UN should play a major role towards international peace in cyber space. Discussants noted cyber security developments within UN fora, including: (1) the General Assembly resolution '*The Right to Privacy in the Digital Age'* tabled in the third committee by Brazil and Germany in 2013, (2) anti-crime mutual legal assistance conventions that could mandate CERT-CERT information sharing, and (3) the ongoing GGE process.

Participants looked forward to forthcoming GGE sessions. Some questioned the utility of discussing how international humanitarian law applies in cyber space given the inherent attribution problems and was concerned that it might send out wrong political signal of cyber war being legalized, suggesting instead to focus first on deliberating rules of state behaviour to prevent cyber war. Others noted the GGE's mandate was advisory rather than strictly inter-governmental, and the UN's generally limited involvement of non-state stakeholders. Some questioned whether the UN's 'one state, one vote' decision process rendered it too cumbersome to address fast moving cyber issues, and another noted challenges implied when one state's position was inconsistent between fora. There were also calls to segment cyber issues across fora.

It was noted that the UN is one possible venue, but not the only venue, for discussion of internet governance issues. Many referred to the need for internet governance to be democratic, transparent, multilateral and multi-stakeholder, and emphasised that 'multilateral' and 'multi-stakeholder' are compatible, complementary features that reinforce each other. Delegates also highlighted: (1) NETmundial, and (2) ICANN's consultations, where government, business and citizens could contribute to discussion of technical issues. One participant noted governments' current *advisory* role in governing ICANN, and welcomed the US' intent to transition key internet

domain name functions to the global multi-stakeholder community. There was also a call to extend the IGF's mandate and funding, and that developing countries' participation would benefit from extra resources.

One speaker referenced calls by Brazil's president for the UN to play a leading role in regulating state behaviour in relation to new technologies, while another noted that broader UN roles would need first to be mandated by member states.

Session IV: Interaction and Cooperation between National Level Actors

China Institute of International Studies
Associate Research Fellow

Speaking in a private capacity, the representative expounded the importance of international cooperation, with whom and on which issue to cooperate, as well as possible next steps.

The speaker stressed the importance of international cooperation for resilience against cyber crime, terrorism and warfare. The complexity of the stakeholder landscape was outlined, with cyber issues touching the individual, community, entity and government agency levels, as well as being multi-dimensional, i.e. economical, security, geographical and political. The delegate argued that states were uniquely authorised, resourced, obligated and positioned to take the lead coordinative role in international cooperation on cyber issues.

Four types of cooperation were suggested: (1) technology transfer to develop basic information infrastructure for developing countries, (2) legal cooperation against cyber crime, (3) confidence-building measures, and (4) formulation of international rules of internet governance and state behaviour. On the latter, the speaker noted the difficulties of applying existing international laws to cyber space, and called for new laws or treaties. The participant also noted China's early efforts to discuss the issue of information security in cyber space, highlighting the SCO's 2011 *International Code of Conduct for Information Security(A/66/359)*.

Looking forward, the speaker called for the 2014/15 GGE to clarify concepts, agree norms and rules on cyber conflict and for enhanced regional cooperation, including on emergency response and in ARF and APCERT.

Thailand
Director, Office of Security, Electronic Transactions Development Agency

The representative from ThaiCERT highlighted trusting international cooperation, explained challenges in coordinating national responses to cyber threats, and outlined measures to overcome them.

The delegate reported that ThaiCERT already had trustful working relationships with other national CERTs: over 90% of reported cyber incidents in 2013 were conveyed by international partners. The speaker explained how such cooperation had been reached within CERT fora, both international (FIRST) and regional (APCERT, OIC-CERT, ENISA, LACNIC). Importantly, technical-level cooperation and trust arose as a result of direct contact, and without government intervention or coordination with state diplomatic channels.

National challenges included: (1) the wide range of stakeholders, (2) aligning terminology and technical understanding between technical and policy levels, (3) clarifying the roles and responsibilities across stakeholders and stipulating national points of contact, (4) establishing chains of command (e.g. between the government and critical infrastructure providers, or central and local government agencies), and (5) increasing the quantity and quality of technical human resource personnel.

The speaker proposed addressing these challenges by putting in place a strategy to include governance structures, legislation and mandating collaboration, building capacity on awareness/technical understanding and rehearsing security drills, and information sharing management systems and protocols.

USITO
President and Managing Director

Representing a consortium of US hardware/software ICT and telecommunication companies, the USITO delegate highlighted the Internet's value, challenges when addressing data security, and next steps in internet governance.

The speaker noted that despite its youth, the internet platform has already transformed the world socially and economically. The ITIF predicts that by 2025 half of global GDP will derive from ICT, including internet industries. The representative emphasised ICT's potential for addressing social challenges and driving growth in developing countries, and called for any future governance frameworks to safeguard innovation and growth-enabling features of the internet platform, including free flowing information and e-commerce.

The delegate argued that data security is user (not product) centred, and that regulations discriminating against ICT products based on their origin do not necessarily enhance data security. In fact, they can be counterproductive, given the globally integrated ICT industry. The speaker also highlighted an ongoing explosion in network complexity, and governments' inability to manage such growth alone.

Looking forward, the representative proposed continuing the multi-stakeholder approach to ensuring data security – in particular, using public-private partnerships to build on existing initiatives, such as the US NIST, World Semiconductor Council and APEC Cross-Border Privacy Rules framework, and adapt rapidly to emerging trends. The delegate argued that continued internet benefits would flow if states facilitated innovation through transparent regulatory frameworks which safeguard intellectual property – and urged governments to protect the 'goose laying the golden eggs'.

CNCERT (China)
Senior Engineer

The representative explained cyber threats facing China, and successful international cooperation to address them. The speaker introduced CNCERT as an NGO operating under China's Ministry of Industry and Information Technology.

The speaker underscored that China's 618 million internet users were vulnerable to hackers – thanks to both users' lack of knowledge and vulnerable loopholes in application software. The participant noted that alongside 926 incoming complaints (mainly complaints of worms and phishing), CNCERT itself filed 5498 complaints against users outside China (mainly phishing of Chinese banks).

The delegate outlined CNCERT's engagement in successful international cooperation to address these threats, via relationships with 59 countries and 127 organisations. Among other actions taken, CNCERT shared information on loopholes and malicious code samples (including with Microsoft and Google), and helped other countries defining responses channels/processes and running emergency response drills. Regional cooperation was also highlighted, with China, Japan and Republic of Korea signing the Three-Party Cyber Security Memorandum and CERT working group in 2011 (authorising CERT-CERT information sharing and respond efficiently to cyber attacks). An example was given where CNCERT and KoreanCERT collaborated to trace a cyber attack perpetrator's IP address, building bilateral trust.

The speaker affirmed China's commitment to international cooperation (including on research and development), calling for others to join in the practical effort to address cyber threats and emergency response.

Discussion

Discussion focused on how to build trust between stakeholders, and the protection of critical infrastructure.

Delegates questioned how users' trust could be regained, given various revelations and the possibility that some ICT companies know more about users' online activity than the users themselves. In addition, concerns about trojan hardware were expressed. One participant emphasised the importance of involving private sector actors in any solution, proposing that governments work with private companies to ensure transparency and legislative frameworks conducive to maintaining customer trust. Another speaker queried how governments could protect critical infrastructure from disruptive cyber incidents. Besides isolating and shutting down affected networks, suggestions included: (1) training infrastructure owners in safeguarding against attacks, (2) building sector-specific CERTs, and (3) relevant legal measures.

Session V: Regional Dialogue, Cooperation and Capacity Building

Malaysia
Principal Assistant Secretary, Cyber and Space Security Division, National Security Council, Prime Minister's Department

The representative presented an overview of cooperation in cyber security undertaken by ASEAN. The presentation conveyed information on ASEAN bodies responsible for cyber security and fighting cybercrime efforts under the ASEAN three pillars: ASEAN Political-Security Community (APSC), ASEAN Economic Community (AEC) and ASEAN Socio-Cultural (ASCC). They are the ASEAN Ministerial Meeting on Transnational Crime (AMMTC)/ SOMTC, the ASEAN Regional Forum (ARF), ASEAN IT and Telecommunications Ministers' Meeting (TELMIN)/ ASEAN Senior Officials Meeting on IT and Telecommunications (TELSOM), ASEAN Telecommunications Regulatory Council (ATRC) and ASEAN Senior Officials Meeting on Social Welfare and Development (SOMSWD). The delegate called for synergy between national, regional and international collaboration, and reaffirmed that the country will continue to play an active role in enhancing mutual understanding and strengthening cooperation in the region.

Republic of Korea
Deputy Director, International Security Division, Ministry of Foreign Affairs

The representative explained the country's cyber situation, pragmatic response, and international engagement. The delegate noted that ROK is one of the most hyper-connected countries in the world, yielding significant economic benefits that the government is planning to continually sustain. However, their heightened cyber vulnerabilities are illustrated by previous cyber attacks that paralysed broadcasting and financial systems, as well as significant and increasing cyber crime and online bullying. The speaker noted ROK's pragmatic response to such threats, such as removing online anonymity to deter users from making malicious comments.

The representative explained motivations for international engagement on cyber security issues, which include addressing international cyber attacks, learning from other countries and sharing development experiences. The delegate described the 2013 Seoul conference on cyber space, which was a multi-stakeholder consultation involving over 1,800 participants from 87 countries which resulted in greater awareness of the need for international cooperation and capacity building on cyber issues, and crystallised international consensus in the outcome document. The speaker also outlined ROK's other international efforts to promote cyber security, including in processes under the GGE, Hague Nuclear Security Summit, the ARF, and MIKTA. Practical measures were also described, including law enforcement and CERT-CERT cooperation, including a cooperation Memorandum of Understanding between ROK's, Japan's and China's CERTs.

China National Institute of Network and Information Security
Director

The representative explained the rationale for regional cooperation, outlined challenges and proposed ways of rebuilding trust.

The participant noted that although cyber security was often cast as a global problem, in practice it is mostly regional. In Asia, most cyber threats are regional, arising from regional historical disputes and criminal networks. Cooperation at the regional level is also more timely, effective and economical than at the international level due to closer time zones and geographical proximity. The speaker argued that APCERT is a successful model of regional cooperation because the framework is built on existing sub-networks of multilateral cooperation, such as China-Japan-Korea network and ASEAN-China network.

The speaker also noted that effective CERT-CERT cooperation and trust was increasingly under threat. The delegate attributed this to: (1) increased attention by government to CERT actions (with bureaucratic control sometimes slowing down information sharing and response, which was previously achieved via direct CERT-CERT communication), and (2) politicisation of cyber space, with rising interstate accusations implicating CERTs, which are increasingly identified with governments.

Arguing that international cyberspace had been fragmented, the delegate proposed rebuilding trust from the regional level, including via strengthening each country's technical capacity, enhancing cooperation in education and training, transparency measures and by setting 'red lines' of state behaviour in cyberspace (e.g. over critical infrastructure).

Australia
Assistant Secretary, International Security Division, Department of Foreign Affairs and Trade

The representative highlighted the urgent need for the development and implementation in this region of cyber confidence-building measures, recognising that the development of norms was a long-term endeavour that would not yield immediate, practical results. The speaker argued that rising interstate security interest and competition in cyber space have created the need for practical steps to reduce misperceptions, miscalculation, and potentially escalation to conflict, taking into account the unique attributes of cyber events, especially the lack of external 'observables'.

Noting that regional organisations are well suited to developing and operationalising such steps, the speaker outlined the ARF's progress in mandating, formulating and implementing cyber confidence-building measures. The speaker traced ARF policy evolution from a focus on cyber-terrorism in 2006, through the adoption of a second Ministerial Statement on Ensuring Cooperation in Cybersecurity in 2012, to the development of a work plan on practical cooperation on confidence-building measures, expected to be adopted in 2014. ARF cyber-CBM implementation was also explained, with examples given of two ARF workshops that raised awareness on this agenda, but also highlighted challenges, including capacity gaps in interagency coordination within states, varying levels of understanding of cyber issues between policy and technical communities, and the importance of cyber points of contact to facilitate regional communication between governments to prevent cyber events escalating. Whilst noting regional disparity in capacity, it was emphasised that confidence building needed to go hand in hand with capacity building, and should complement and build upon existing structures.

The speaker drew attention to Australia's role as chair of the 2012/13 GGEs on cyber, and emphasised that Australia regards the framework of existing international law as the starting point for any discussion of norms of state behaviour in cyberspace. Building on the 2013 consensus report, the speaker urged the 2014/15 GGE to focus on the

important international task of elaborating how existing international law, including the UN Charter and international humanitarian law, apply to state behaviour in cyberspace.

UK

Assistant Director, International Relations Office for Cyber Security and Information Assurance, Cabinet Office

The representative of the UK's International Relations Office for Cyber Security and Information Assurance explained the UK's cooperative approach towards regional confidence-building measures, capacity building and future dialogue on cyber security issues.

The delegate expounded a regional OSCE initiative, two years in the making, which agreed a range of voluntary CBMs to promote transparency and cooperation between participating States. Citing success factors of concerted focus, will and flexibility in helping 57 OSCE states forge ministerial agreement on CBMs, the representative noted that implementation now depends on state action.

On capacity building, the speaker outlined the UK FCO's £2 million per year International Cyber Security Capacity Building programme, which aims to help develop national cyber security strategies, cybercrime capabilities, legislation and CERTs, especially among developing countries. The multi-region, multi-partner fund has supported a global information exchange platform, as well as igniting and incubating regional initiatives in Africa and other regions.

The delegate expressed hope that future international dialogue would be multi-stakeholder (like the London-Budapest-Seoul-Netherlands Conference series on Cyberspace), better informed via training assistance provided through ICT4Peace, and fruitful in developing common understandings and norms of behaviour .

Discussion

During discussion, representatives outlined national positions, noted cyber-crime as a possible area for joint work, and discussed focus points for cyber capacity building.

One representative also outlined the South American regional cooperation architecture, giving detail on initiatives within Mercosur and UNASUR. On Mercosur, the delegate referred to: (1) Mercosur states' decision in July 2013 to cooperate to ensure cyber security, individual privacy, human rights and sovereignty, (2) Mercosur's joint demarche to the UN Secretary General in August 2013 conveying the region's prioritisation of cyber security issues, and requesting cyber espionage prevention mechanisms and sanctions for cyber security breachers, and (3) the formation of a Mercosur cyber security working group. The speaker also noted that in August 2013, UNASUR's Heads of States: (1) declared cyber espionage and telecommunication interception to be security threats, violations of human, civil and political rights and breaches of sovereignty and international law, and (2) instructed UNASUR Councils to coordinate efforts for safer telecommunications, promoting regional technologies, digital inclusion and protection of human rights.

Another highlighted African regional initiatives, including: (1) ongoing harmonisation of legal frameworks within SADC, focusing on electronic transactions, personal data protection and cyber-crime; (2) future harmonising of laws and regulations following adoption of African Union's Convention on Cyber Security and Personal Data Protection in May 2013 and (3) intra/inter-regional international cooperation and capacity building with *inter alia* EU, USA and China including at the operational level.

One speaker highlighted its country's support for an open, interoperable, secure and reliable internet, and conviction that free flowing information remains crucial for the Internet's success. The delegate acknowledged the successes of the two most recent GGEs, and expressed hope for similar global progress in the forthcoming GGE process, but asserted reservation over that the proposed *International Code of Conduct for Information Security*, and

its concept of 'information security', was equivalent to state censorship of content and was inconsistent with the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights.

International confidence-building measures were cited as a key priority for one delegate, as were activities such as helping develop national cyber strategies, CERT capabilities and anti-crime legislation, investigation capabilities, and formal/informal law enforcement international cooperation. Practical advantages of working with regional organisations were highlighted, including capacity-building activities across multiple continents including OSCE, OAS, ASEAN and ARF. Various areas were identified as a high potential area for initial cooperation and trust building, including: (1) cooperation between CERTs, (2) communication between governments and amid regional organisations, and (3) collective cooperation on tackling cyber crime, including among law enforcement agencies.

Another participant echoed calls for international cooperation against cyber crime and cyber terrorism, and proposed that anti-crime anti-terrorism approaches and principles could be extended geographically and to other issues, including respect for sovereign jurisdictions and regulations.

The meeting concluded with a reiteration of the goals of the workshop, which was to bring together various stakeholders to facilitate discussion on a matter of pressing concern and enhance mutual trust. There was general agreement that this goal was achieved and important information had been exchanged. It is hoped that the results of the workshop will contribute to the ongoing dialogue on the issue and has provided some interesting food for thought on the ways forward.

ANNEX I: List of Acronyms used in this Report

AMMTC	ASEAN Ministerial Meeting on Transnational Crime
APCERT	Asia Pacific Computer Emergency Response Team
APEC	Asia-Pacific Economic Cooperation
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
ATRC	ASEAN Telecommunication Regulators' Council
CBM	Confidence-building Measure
CERT	Computer Emergency Response Team
CERT|CC	Computer Emergency Response Team Coordination Centre
CNCERT	China's Computer Emergency Response Team
ENISA	European Union Agency for Network and Information Security
EU	European Union
FCO	Foreign and Commonwealth Office
GAC	Governmental Advisory Committee
GDP	Gross domestic product
GGE	Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IISS	International Institute for Strategic Studies
ITIF	Information Technology and Innovation Foundation
ITU	International Telecommunication Union
LACNIC	Latin America and Caribbean Network Information Centre
MIKTA	Mexico, Indonesia, Republic of Korea, Turkey, and Australia
NCPO	National Cyber Policy Office
NIST	National Institute of Standards and Technology

OAS	Organization of American States
OIC-CERT	Organisation of The Islamic Cooperation-Computer Emergency Response Team
OSCE	Organization for Security and Co-operation in Europe
ROK	Republic of Korea
SADC	Southern African Development Community
SCO	Shanghai Cooperation Organization
SOMTC	ASEAN Senior Officials Meeting on Transnational Crime
TELMIN	ASEAN Telecommunications and IT Ministers Meeting
UN	United Nations
UNASUR	Union of South American Nations
UNIDIR	United Nations Institute for Disarmament Research
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UNRCPD	United Nations Regional Centre for Peace and Disarmament in Asia and the Pacific
USITO	United States Information Technology Office
WCIT	World Conference on International Telecommunications

ANNEX II: Workshop Agenda

Opening Session
Distinguished Speakers:
H.E. Mr. LI Baodong, Senior Vice Foreign Minister of China
Mr. Jarmo SAREVA, Deputy Secretary-General of the Conference on Disarmament and Director of Geneva Branch, UNODA
Co-Chairs:
Mr. FU Cong, Coordinator for Cyber Affairs, Ministry of Foreign Affairs, China
Ms. Sharon RIGGLE, Director, UNRCPD

Session I: Cyberspace Policies and Emerging Challenges
Moderator:
Ms. Sharon RIGGLE, Director, UNRCPD
Speakers:
Mr. Rohana PALLIYAGURU, Manager Operations & Principal Information Security Engineer, Sri Lanka CERT|CC
Ms. Georgina Elizabeth SARGISON, Policy Officer, International Security and Disarmament Division, Ministry of Foreign Affairs & Trade, New Zealand
Amb. SHIMMI Jun, Ambassador in charge of UN Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Japan
Mr. Mureed HUSSAIN, Director of Cyber Security, Ministry of Defence, Pakistan

Session II: Formulation of International Rules and Norms in Cyberspace
Moderator:
Mr. Dennis DLOMO, Coordinator for Intelligence, National Intelligence Coordinating Committee, South Africa
Speakers:
Mr. FU Cong, Coordinator for Cyber Affairs, Ministry of Foreign Affairs, People's Republic of China
Mr. Martin FLEISCHER, Head of International Cyber Policy Coordination Staff, German Federal Foreign Office
Mr. RADOVITSKIY Alexander, Aide to Special Representative of the President of the Russian Federation on International Cooperation in the Field of Information Security
Mr. KUEK Yu-Chuang, Vice President and Managing Director, ICANN

Session III: The Role of the United Nations in Promoting Dialogue on Cyber Security
Moderator:
Mr. Jarmo SAREVA, Deputy Secretary-General of the Conference on Disarmament and Director of Geneva Branch, UNODA
Speakers:
Mr. Marco OBISO, Cybersecurity Coordinator, ITU
Mr. John SANDAGE, Director, Division for Treaty Affairs, UNODC
Mr. Benjamin BASELEY-WALKER, Programme Lead, UNIDIR
Mr. Nigel INKSTER, Director of Transnational Threats and Political Risk, **IISS**
YANG Mingjie, Vice President, China Institutes of Contemporary International Relations

Session IV: Interaction and Cooperation between National Level Actors
Moderator:
Mr. Martin FLEISCHER, Head of International Cyber Policy Coordination Staff, German Federal Foreign Office
Speakers:
XU Longdi, Associate Research Fellow, China Institute of International Studies
Dr. Soranun JIWASURAT, Director, Office of Security, Electronic Transaction Development Agency, Thailand
Mr. Matt ROBERTS, President and Managing Director, USITO

JI Yuchun, Chief Engineer, Department of Administration and Operation, CNCERT, China

Session V: Regional Dialogue, Cooperation and Capacity Building

Moderator:
Amb. Daniel STAUFFACHER, President, ICT4Peace

Speakers:
Ms. Shariffah Rashidah SYED OTHMAN, Principal Assistant Secretary, Cyber and Space Security Division, National Security Council, Prime Minister's Department of Malaysia
Ms. Jooyeon Ellen KANG, Deputy Director, International Security Division, Ministry of Foreign Affairs, ROK
DU Yuejin, Director, National Institute of Network and Information Security, China
Mr. Ian BIGGS, Assistant Secretary, International Security Division, Department of Foreign Affairs and Trade, Canberra, Australia
Miss Olivia PRESTON, Assistant Director, Office for Cyber Security and Information Assurance, Cabinet Office, UK

Closing Session

Speakers:
Ms. Sharon RIGGLE, Director, UNRCPD
Mr. FU Cong, Coordinator for Cyber Affairs, Ministry of Foreign Affairs, China

ANNEX III: List of Participants

Mr. Ian BIGGS, Assistant Secretary, International Security Division, Department of Foreign Affairs and Trade, Canberra, Australia

Ms. Natasha KASSAM, Second Secretary, Australian Embassy, Beijing

Mr. Claudio GARON, Minister Counsellor, Brazilian Embassy , Beijing

Mr. Rafael LEME, First Secretary, Brazilian Embassy , Beijing

Ms. Noor Airah ABDUL RAHMAN, ICT Acting Director, Ministry of Foreign Affairs and Trade, Brunei

Pol. Lt. Col Hay MAKARA, Chief of Anti Cybercrime Bureau, Internal Security Department, General Commissariat of Cambodian National Police, Ministry of Interior, Cambodia

FU Cong, Coordinator for Cyber Affairs, Ministry of Foreign Affairs, China

LI Chijiang, Director, Office for Cyber Affairs, Ministry of Foreign Affairs, China

CHEN Kai, Secretary General, China Arms Control and Disarmament Association

WANG Juan, Director, Bureau of News, the Publicity Department of the CPC Central Committee, China

HU Xiao, Director, the Cyber and Information Security Coordination Department, the State Internet Information Office, China

CAI Donghai, Director, Internet Exchange and Cooperation Department, the State Internet Information Office, China

LI Xuelin, Deputy Director General, Bureau of Communication Security, Ministry of Industry and Information Technology, China

LIU Bochao, Associate Consultant, Division of Network Security Administration, Bureau of Communication Security, Ministry of Industry and Information Technology, China

GUO Qiquan, Chief Engineer, Cyber Security Department, Ministry of Public Security, China

LIU Ying, Deputy Director, Cyber Security Department, Ministry of Public Security, China

Col. XUE Xiaodong, Foreign Affairs Office of Ministry of National Defence, China

YANG Mingjie, Vice President, China Institutes of Contemporary International Relations

TANG Lan, Deputy Director, China Institutes of Contemporary International Relations

XU Longdi, Associate Research Fellow, China Institute of International Studies

WU Chunsi, Director, Shanghai Institutes for International Studies, China

LU Chuanying, Research Fellow, Shanghai Institutes for International Studies, China

LIU Yue, Director, China Academy of Telecommunication Research of Ministry of Industry and Information Technology

HE Jia, Analyst, China Academy of Telecommunication Research of Ministry of Industry and Information Technology

DU Yuejin, Director, National Institute of Network and Information Security, China

WANG Jun, Chief Engineer, China Information Technology Security Evaluation Center

LI Jing, Director of Research and Analysis Department, China Information Technology Security Evaluation Center

LU Zhi'an, Deputy Director, Academy of Military Science, China

XU Manshu, Associate professor, Center for Crisis Management, National Defence University, China

WANG Aiping, Associate Research Fellow, China Institute for International Strategic Studies

SHI Xiansheng, Vice Secretary General, Internet Society of China

ZHONG Rui, Deputy Director, International Cooperation Department, Internet Society of China

JI Yuchun, Chief Engineer, Department of Administration and Operation, CNCERT, China

YAN Hanbing, Deputy Director, Department of Administration and Operation, CNCERT, China

XU Yuan, Officer, Department of Administration and Operation, CNCERT, China

QU Bing, Vice President, Qihoo 360 Technology Co., Ltd.

LIU cong, Manager of Government Affairs, Tencent

SUN Zihan, Manager of Government Affairs, Tencent

YANG Hongyu, Huwei Technologies Co., Ltd

Ms. Myriam PAVAGEAU, First Secretary, French Embassy, Beijing

Mr. Martin FLEISCHER, Head of International Cyber Policy Coordination Staff, German Federal Foreign Office

Mrs. Anke SCHLIMM, Counsellor, German Embassy, Beijing

Mr. Jürgen SCHUMACHER, German Embassy, Beijing

Mr. Vinod K. JACOB, Counsellor, Indian Embassy, Beijing

Mr. R. Madhu SUDAN, Second Secretary, Indian Embassy, Beijing

Mr. Gince K. MATTAM, Third Secretary, Indian Embassy, Beijing

Amb. SHIMMI Jun, Ambassador in charge of UN Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Japan

Mr. KAWAGUCHI Kohei, Deputy Director, Foreign Policy Bureau, Japan

Lt. Col. Artem ZAKARDOTSEV, Deputy Chief, State Committee on National Security, Kyrgyzstan

Mr. Khamphanh SOUVANNAKHA, Deputy Director General of LAONATIONAL INTERNET CENTER, Ministry of Posts and Telecommunications Laos PDR

Ms. Shariffah Rashidah SYED OTHMAN, Principal Assistant Secretary, Cyber and Space Security Division, National Security Council, Prime Minister's Department of Malaysia

Ms. Georgina Elizabeth SARGISON, Policy Officer, International Security and Disarmament Division, Ministry of Foreign Affairs & Trade, New Zealand

Mr. Mureed HUSSAIN, Director of Cyber Security, Ministry of Defence, Pakistan

Ms. Jooyeon Ellen KANG, Deputy Director, International Security Division, Ministry of Foreign Affairs, ROK

Mr. RADOVITSKIY Alexander, Aide to Special Representative of the President of the Russian Federation on International Cooperation in the Field of Information Security

Mr. SEROV Oleg, Counsellor, Russian Embassy, Beijing

Mr. ULIANOV Alexey, Third Secretary, Russian Embassy, Beijing

Mr. Dennis DLOMO, Coordinator for Intelligence, National Intelligence Coordinating Committee, South Africa

Ms. Irene MOETSANA, Head of National Communications, State Security, South Africa

Mr. Rohana PALLIYAGURU, Manager Operations & Principal Information Security Engineer, Sri Lanka CERT|CC

Mr. Kadamjon SAFIEV, Head of IT Department, Executive Office of the President of the Republic of Tajikistan

Dr. Soranun JIWASURAT, Director, Office of Security, Electronic Transaction Development Agency, Thailand

Chotirat KOMARADAT (Ph.D), First Secretary, International Security Unit, Ministry of Foreign Affairs, Thailand

Miss Rawinnipa KARIN, Office of the National Security Council, Thailand

Engr. Virgilio T. SIBUG, Officer-in-Charge, Network Computing and Infrastructure Mngt Division, Information and Communications Technology Office, Department of Science and Technology, The Philippines

Mr. Federico Heriberto C. DELA LLANA, Information Technology Officer, Department of Science and Technology, The Philippines

Mr. Thomas DUKE, Deputy Director, Office of the U.S. Department of State's Cyber Coordinator

Mr. William FLENS, First Secretary, U.S. Embassy, Beijing

Miss Olivia PRESTON, Assistant Director, Office for Cyber Security and Information Assurance, Cabinet Office, UK

Mr. Craig PATCHETT, Second Secretary, British Embassy, Beijing

H.E.Mr. KURBANOV Daniyar, Ambassador Extraordinary and Plenipotentiary, Uzbekistan Embassy, Beijing

Mr. Mattias LENTZ, Minister Counsellor, Delegation of the European Union to China

Mr. Svilen GEORGIEV, Second Secretary, Delegation of the European Union to China

Mr. Jarmo SAREVA, Deputy Secretary-General of the Conference on Disarmament and Director, UNODA, Geneva Branch

Ms. Sharon RIGGLE, Director, UNRCPD

Mr. Quintin CHOU, Peace and Disarmament Officer, UNRCPD

Ms. Essi HYNNINEN, Peace and Disarmament Officer, UNRCPD

Mr. Marco OBISO, Cybersecurity Coordinator, ITU

Mr. John SANDAGE, Director, Division for Treaty Affairs, UNODC

Mr. Benjamin BASELEY-WALKER, Programme Lead, UNIDIR

Mr. KUEK Yu-Chuang, Vice President and Managing Director, ICANN

Mr. SONG Zheng, Head of China, Beijing Engagement Center, ICANN

Mr. Nigel INKSTER, Director of Transnational Threats and Political Risk, IISS

Amb. Daniel STAUFFACHER, President, ICT4Peace

Mr. Matt ROBERTS, President and Managing Director, USITO