UNIDIR

UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict

UNIDIR RESOURCES

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to the variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and governments. UNIDIR's activities are funded by contributions from governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The views expressed in this publication are the sole responsibility of UNIDIR. They do not necessarily reflect the views or opinions of the United Nations or UNIDIR's sponsors.

www.unidir.org

UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict

Seminar Report

10 February 2014, Geneva, Switzerland

Organized with support from the Governments of Australia, Germany, and Switzerland.

UNIDIR held its second Cyber Stability seminar entitled "Preventing Cyber Conflict" on 10 February 2014 in Geneva, Switzerland. The seminar was organized with the support of the governments of Australia, Germany, and Switzerland. The seminar presented an opportunity for states and relevant stakeholders to discuss how to take pragmatic steps towards a more stable and predictable cyber environment. With particular attention paid to the risks of escalation in cyber conflicts, the seminar addressed the growing need to develop mechanisms for discussion, education, and constructive engagement on how to improve cyber stability in the multilateral context.

Introduction: The Cyber Stability Context

With the emergence of the Internet as a global infrastructure for economic and social development, business, and as a new tool for politics, espionage, and military activities, there is growing international concern regarding the potential for the use of information and communications technologies (ICTs) in conflict. The 2010 and 2013 Reports of the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security recommended steps to reduce the risk of misperceptions resulting from ICT disruptions, among them the consideration of "Confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs".[1]

There is now a realization at the international level that the need for such action is becoming ever more pressing given the growing pervasiveness of cyberspace applications throughout government activities, military planning, and operations, industrial and civil infrastructure, and financial systems. While cyberspace offers immense benefit through its capacity to

1 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/65/201 of 30 July 2010.

convey information globally and at great speed, such pervasiveness presents an increased number of threats for governments, militaries, businesses, and the general public. These challenges include state-to-state cyberattacks as well as attacks on a state by non-state actors (which may be either fully independent of tacitly supported by a state). Such attacks could also be launched from or routed through proxy states.

Given the well-known technical difficulty in attributing identity to the perpetrators of cyberattacks, the possibility of such state-on-state conflict utilizing ICTs could contribute to strategic instability and raise the risk for misperception in times of crisis. Given the fact that military and civil users rely on the same infrastructures, the potential negative impacts on civil society and infrastructures could be severe. In light of these developments, there is a growing need to develop mechanisms for discussion, education, and constructive engagement on how to improve cybersecurity in the multilateral environment. Enhancing transparency, confidence, and predictability in the cyber realm is a central foundation for future progress. As such, this seminar once again focused on the concept of cyber stability—what it means to different actors, what measures need to be put in place to work towards achieving a stable cyber environment, and what upcoming initiatives may contribute to that goal.

PROCEEDINGS

Seminar Chair

- **Mr. Ben Baseley-Walker**, Programme Lead, Emerging Security Threats, UNIDIR

Welcoming Remarks

- **Ms. Theresa Hitchens**, Director, UNIDIR
- **Mr. Michael Møller**, Acting Director-General, United Nations Office at Geneva
  "The New Strategic Balance: Making Space for Cyber Stability"
- **Mr. Ben Baseley-Walker**

In her opening comments, Ms. Hitchens explained that this seminar provides a unique opportunity to hold a cross-stakeholder discussion on cyber stability. She noted that under her direction, the United Nations Institute for Disarmament Research has consistently supported cross-stakeholder engagement on cyber issues working with key industry players, government offices, and other relevant actors to understand and develop future cyber policy direction that could contribute to a stable and secure cyber environment.

Mr. Møller gave keynote remarks on the rapidly evolving field of cyber technology and how it affects international relations. Mr. Møller explained that the creation of the cyber domain is perhaps the most important game-changer of our time—in 1993, only fifty internet websites existed, by 2011, this number increased to 555 million and will only continue to grow. With this exponential increase in internet activity, cyberattacks and cyber malfeasance are also increasing, and they are becoming more complex and economically detrimental. Some states have now incorporated cyber resources into their defensive arsenal and strategic calculations. Consequently, national, regional, and international efforts are currently underway to assess the risks associated with the militarized uses of cyber resources, and to examine how cyber technology can be addressed under international law.

Mr. Møller felt that Geneva, as the seat of multilateral disarmament and a hub of diplomatic expertise, has a key role to play in providing a forum for the international community to discuss how to build transparency and confidence in the cyber domain and how best to ensure that the Internet and other cyber resources can continue to be used peacefully for the benefit of all United Nations Member States and their citizens. Mr. Møller concluded his speech by affirming that it is imperative that the international community continue to develop understanding on what is acceptable behaviour in cyberspace in order to avoid it becoming an arena for uncontrolled escalation and unintended conflict.

Mr. Baseley-Walker then provided some initial thoughts on the aim of the seminar and explained how cyber-related issues are regarded both within UNIDIR and more broadly in the multilateral context. In his opinion, the biggest hurdle for the international community is defining the terms the "cyber security" and "cyber stability", and what is meant when these terms are used at the multilateral level. At UNIDIR, research focuses on cyber stability rather than security, the latter being used to cover an excessively wide category of activities including combatting credit card theft, child pornography, minor hacking, et cetera. In working towards a stable cyber environment, Mr. Baseley-Walker explained that UNIDIR sees its most effective contribution as supporting dialogue on transparency and confidence-building measures (TCBMs); this is something to which UNIDIR has been dedicated for a number of years as TCBMs can be a positive first step on the way to larger agreements where global consensus is vital.

In the cyber stability conversation, the interconnection of sectors, actors, and areas of governance is extreme and requires extensive dialogue to create mutual understanding. Therefore, when organizing an intra-governmental meeting on cyber stability, one must involve every government department, ministry, and bureau; everyone, including the private sector and private citizens, has a stake in the cyber conversation. To create such broad representation in the context of this meeting, UNIDIR brought together representatives from the research community, various departments of government, international organizations (IOs), and the private sector to facilitate a cross-sectoral dialogue. In this vein, this meeting can contribute to collective understanding and drive the conversation forward in pursuit of a stable cyber environment.

Panel 1: TCBMs in the International Security Context

- **Mr. Karsten Geier**, Head of Division, Arms Control and Disarmament–Communication, New Challenges, Federal Foreign Office, Germany
  "Destroying the Ring Fence: Cyber Stability in Wider International Security Calculus"
- **Ms. Nadezhda Sokolova**, Expert in the Field of Information Security, Ministry of Foreign Affairs, Russian Federation
  "Controlling Escalation: Understanding Cyber Realities"
- **Mr. Tim Maurer**, Research Fellow, Open Technology Institute, New America Foundation
  "Policy Options: TCBMs and Controlling the Proliferation of Cyber Weapons"

Panel 1, "TCBMs in the International Security Context", brought together state and non-governmental organization perspectives on the current status of TCBMs and future steps for multilateral TCBM engagement. The first panellist, Karsten Geier, situated cyber stability in the context of wider security arrangements. He began his presentation with an analogy for the international security system: the system is a pasture, surrounded by a fence, inside

which all states are represented as grazing cattle. Multiple instruments of international law—multilateral and bilateral agreements, norms, rules, principles, and procedures— constitute the fence. Mr. Geier explained that cyber technology broke this fence because it is inherently different than other military technologies or capabilities. Firstly, cyber technology is not limited to military powers around the world nor to state actors—private actors, smaller states, criminals, or terrorists can use cyber technology as a weapon. Secondly, cyber activity is not limited to cyberspace; it can have very physical consequences in other domains. Mr. Geier used two examples to illustrate possible physical consequences—the 2010 Stuxnet virus which disabled and destroyed centrifuges in the Islamic Republic of Iran, and a theoretical virus that disrupts a state's power grid. Going back to his initial model of the security system as a pasture, Mr. Geier asserted that the broken fence has led to two consequences: (1) states can leave the fenced-in pasture and explore cyberspace; and (2) predators—criminals, terrorists committing acts of malfeasance—can now enter the international security system.

Given potential ramifications in the physical world, Mr. Geier explained that the militarized application of cyber technology demands new containment strategies from states and the international community. Traditionally, states could leverage negative consequences or methods of deterrence to achieve strategic goals. However, because it is difficult to accurately attribute the origin of hostile cyber activity, traditional military options are rendered relatively ineffective in situations where cyber technology is militarized. For Mr. Geier, traditional arms control agreements would also not comprehensively address the cyber issue because of the unlimited number of possible actors that can procure computer malware. However, before the international community can pursue policies to mitigate cyber conflict, the threats must be understood. Mr. Geier outlined three possible cyber conflict scenarios:

1. **All-out cyber war**—a case where a cyberattack could wipe out a state's military force, economy, and communication infrastructure. At present, this type of attack is unlikely, however, it should not be ruled out as impossible.
2. **Use of cyber technology in tandem with larger military capabilities**—a case where limited use of cyber technology is part of a warfighting effort. At present, this type of attack is possible and can pose a major, however limited, threat.
3. **Military crisis developing from cyber incident**—a case where a cyberattack might take place between two states with strained relations. In this scenario, there is a high possibility for conflict escalation from the cyber to the physical realm.

Though these scenarios vary greatly in their likelihood, they all raise questions for the international community. Under Article 51 of the Charter of the United Nations, a state is authorized to use self-defence in the event of an armed attack. However, this poses some interesting questions. Is cyber activity considered an armed attack? If a state is authorized, how does the international community determine the threshold for a cyberattack to merit an armed response? Do the international legal principles barring the use of indiscriminate weapons apply if a cyberattack damages critical infrastructure such as hospitals or nuclear power plants? Concluding his presentation, Mr. Geier argued that the international community must address these questions, through the United Nations and regional organizations, in order to develop comprehensive cyber stability agendas.

A central concern of any cyber stability agenda is limiting conflict escalation. Nadezhda Sokolova of the Russian Federation was able to provide a national perspective on escalation, TCBMs, and cyber stability in the international context. Rather than Mr. Geier's three scenarios for cyber conflict, she saw only two—war and peace. For her, escalation of cyber

conflict is dangerous and uncontrollable, thus international dialogue should focus on conflict prevention. An intrinsic part of prevention is creating global consensus on contentious issues, something that Ms. Sokolova felt the June 2013 United Nations Group of Governmental Experts' (GGE) report on developments in the field of information and telecommunications in the context of international security (abbreviated here as the 2013 GGE report)[2] showed was possible in a cyber context through its affirmation that it is in the interest of all states to promote the use of ICTs for peaceful purposes and to prevent ICT-related conflict.[3]

Continuing her presentation, Ms. Sokolova provided an overview of cyber-related developments involving the Russian Federation. Following the success of the previous the GGE on information security, the Russian Federation supported the expansion of the upcoming GGE starting in June 2014 from 15 to 20 experts meeting in four sessions, rather than the previous three. In June 2013, the Russian Federation concluded an agreement and established a working group with the United States of America on TCBMs in cyberspace with the aim to reduce tensions caused by ICT-related malfeasance.[4] The agreement, described by Ms. Sokolova as "unprecedented", calls for information exchange up to a very high level. Ms. Sokolova felt that while these bilateral agreements are important for cyber stability, they cannot by themselves eliminate all threats to international security. To achieve this, devising regional agreements on ICT-related TCBMs—similar to the Shanghai Cooperation Organization's 2009 Agreement on Information Security and the 2013 Organization for Security and Co-operation in Europe's ministerial agreement on a first set of cyber TCBMs (abbreviated here as the 2013 OSCE ministerial agreement)—are logical next steps. She concluded her presentation by affirming that the international community is interested in consensus-driven TCBMs, norms, and principles in cyberspace and that moving away from these processes could bring about scenarios of uncontrollable escalation, or war.

Mr. Maurer provided participants with some potential policy options for controlling the proliferation of cyber weaponry. He began by noting the recent advancements in diplomatic negotiations on cyber stability—the 2013 OSCE ministerial agreement, the bilateral agreement between the Russian Federation and the United States mentioned by Ms. Sokolova, the establishment of a China–United States ICT working group,[5] and various civil, bilateral negotiations at the track-two level. Mr. Maurer saw these advancements as a firm foundation for discussions on the future of cyber stability. However, he explained that if we look at the specific language contained in many of these agreements dealing with TCBMs, they often focus on transparency and information-sharing, both of which do not have an immediate impact on states' cyber capabilities and thus do little to address today's cyber stability concerns. For policymakers, Mr. Maurer posed the following question: how do we make sure cyber-related policy and regulatory reforms succeed both in the short- and long-term?

One possibility Mr. Maurer presented, but did not endorse, was export controls. He illustrated two recent export control-related developments: the Wassenaar Arrangement and the 2014 United States Fiscal Year National Defense Authorization Act section 940 (NDAA 940). The

2 The document is available at www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

3 In the 2013 GGE report, para. 11, "Member States have repeatedly affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. Further progress in cooperation at the international level will require an array of actions to promote a peaceful, secure, open and cooperative ICT environment. Consideration should be given to cooperative measures that could enhance international peace, stability and security. These include common understandings on the application of relevant international law and derived norms, rules and principles of responsible behaviour of States".

4 For more information see www.state.gov/p/eur/ci/rs/usrussiabilat/219086.htm.

5 For more information see www.usito.org/events/events/usito-us-china-ict-annual-reception.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is an export control regime signed by 41 states in 1996. Mr. Maurer focused on the Arrangement's regulation and definition of "intrusion software" as a way of controlling the spread of cyber weaponry or ICT malware: "'Software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures'".[6] The NDAA 940 the development of policy to control the proliferation of cyber weapons both unilaterally and multilaterally. For Mr. Maurer, these export controls represent possible avenues for states and the international community in the regulation of cyber weaponry. However, difficulties with achieving common definitions of terms, the use of those terms in different communities (international organizations versus non-governmental organizations versus governments), and the dual-use nature of ICTs, will continue to pose challenges to limiting the proliferation of cyber weapons.

The discussion following panel 1 centred on the question of involving non-state actors in the cyber stability discussion. One participant asked how non-state actors—specifically those who have the ability to inflict damage on par with that of a state—can be involved. Someone responded to this by noting that the 2013 GGE report answered this question when it established that states are responsible for all cyber malfeasance that originates from their territory. It was also suggested that TCBMs can address these questions and reduce further misunderstandings. In terms of enlarging existing arms control regimes, one participant asked how the international community should define what is meant by a military or civilian cyber capability. They explained that many companies have greater cyber capabilities than some states, thus while political statements are beneficial to the discussion, they do not adequately address all actors in cyberspace. One participant responded by affirming that opening channels of communication between relevant actors and engaging in TCBMs can help clarify this definition and move the conversation forward.

Panel 2: Looking Forward: 2014

- **Ms. Caroline Baylon**, Research Associate, International Security, Chatham House
  "Internet Governance Developments: What They Mean for TCBMs"
- **Mr. Shen Jian**, Counsellor, Permanent Mission of the People's Republic of China to the United Nations, Geneva
  "A Cyber Code of Conduct: The Best Vehicle for Progress?"
- **Col. Aapo Cederberg**, Senior Advisor, Emerging Security Challenges Programme, Geneva Centre for Security Policy
  "Lessons Learned: Developing a Finnish Cyber Security Strategy"

Panel 2, "Looking Forward: 2014", sought to highlight developments in the coming year and contextualize them in relation to current cyber stability conversations. In her presentation on internet governance, Ms. Baylon began by explaining that discussions on internet governance have two parts—policy aspects and technical aspects. The policy-related aspects examine who should have power, who has legitimacy, who are the stakeholders, et cetera. The technical-related aspects focus on, for example, the Domain Name System (DNS) and TCP/IP arrangements. While her presentation focused on policy, Ms. Baylon asked participants to not discount the significance of technical details because decisions made in that domain have important policy ramifications.

6 "Definitions of Terms Used in These Lists", p. 209, category 4. Available at www.wassenaar.org/controllists/index.html.

For Ms. Baylon, the following three cases of fragmentation represent some of the major debates within internet governance circles—they deserve special attention when outlining relevant developments in 2014. The first deals with the question of who should manage the various entities that make up the internet: the current major "manager" is the Internet Corporation for Assigned Names and Numbers (ICANN), a private, non-profit organization based in the United States that allocates IP addresses and manages the DNS; the other potential "manager" could be the International Telecommunication Union, a United Nations agency that deals with ICT-related issues. The second case of fragmentation is between an Internet based on the multi-stakeholder model versus the national sovereignty model. Ms. Baylon saw this discussion polarized between states that favour an "open" Internet and those that do not, with a variety of undecided states in the centre. She hypothesized that the future of this particular discussion might be determined by alliances made with the undecided states. The last case of fragmentation involves determining the United States' position in the internet governance debate. Ms. Baylon sees a tension between the United States' historic commitment to democracy and an open, multi-stakeholder Internet versus some controversial internet governance stances the US government has recently taken. For Ms. Baylon, a stable and clear American position could help clarify understanding and elucidate potential policy options for the international community.

In determining a way forward in these cases of fragmentation, Ms. Baylon provided a series of recommendations. For the first case, she recommended that ICANN improve accountability and transparency in their decision-making process. For the second, the multi-stakeholder model should prevail and include all stakeholders including the technical community, economic actors, government, and civil society. For the last case, Ms. Baylon saw the United States needing to rebuild international trust after the 2013 NSA PRISM revelations. In all discussions and processes, she supported increased inclusion of developing states.

According to the next panellist, perhaps one of the greatest potential shifts in the cyber stability conversation is the drafting of an international code of conduct (CoC) for cyber activities, originally proposed in 2011 by the People's Republic of China and the Russian Federation, with the support of Tajikistan and Uzbekistan. In his presentation, Mr. Shen explained why the international community needs a CoC and how it might be structured and advanced. In his view, the rapid development of ICTs brings benefits to all, however with these new technologies come new challenges. Pursuing cyber stability involves the security and development interests of all actors in the international community and therefore, the stated purposes of a CoC would be to achieve a consensus on the norms, rules, rights, and responsibilities of states in cyberspace, to promote cooperation and to address commonalities and challenges.

Mr. Shen argued that a CoC was indeed the best way forward for progress on cyber stability but he stressed that it is only the beginning of the process—a CoC would provide a solid platform to facilitate subsequent discussions. At the state level, he believes that governments should play the lead role in determining a state's direction, while allowing for private sector input. In his conceptualization, a CoC would constitute the most important TCBM the international community can establish. Mr. Baseley-Walker affirmed this last point by saying that CoCs are useful frameworks around which the international community can structure other TCBMs.

Looking forward, some states may develop or currently are developing national cyber strategies; since 2013, Finland has been developing its own and the final panellist, Col. Aapo Cederberg, expanded on its methodology and development. He explained that when

national policymakers were developing a Finnish national strategy, they examined other states' cyber policy choices. With the recognition that cyber malfeasance affects all aspects of society, they went on to develop an approach that focused on possible projected damages to Finland. In lieu of an internationally recognized definition for cyber security, he explained that Finland developed its own: "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured". For Finnish policymakers, defining the term established the parameters for addressing the problem. Once policymakers could enunciate the goal—a high level of cyber security and preparedness—they could better direct strategy. The strategy involved identifying threats, performing a risk analysis, establishing the vulnerabilities and possible disturbances, assessing the impacts on society, and determining the best way to pre-emptively prepare. Col. Cederberg explained that by 2016 Finland expects to be the global forerunner in cyber threat preparedness and management thanks in large part to its Cyber Security Strategy.

The discussion period that followed this panel touched on a variety of subjects. One participant challenged the assertion that governments should lead state direction in cyberspace and cyber governance; this participant argued that cyberspace is not only the purview of governments but that companies and individuals have a vital stake and deserve a greater voice. There was a question of how states planned to include non-state actors in the information security CoC drafting process, to which one participant responded that their state established an inter-agency working group that involved the private sector—from their perspective, this had been a positive development and could serve as a model for future private sector–government dialogue. Another participant inquired about a CoC's relationship to international humanitarian law, such as the principle of non-discrimination. If was made clear that a CoC would be open to input and that the United Nations should play a role in facilitating that.

Mr. Baseley-Walker concluded the panel by illustrating a central challenge of developing comprehensive cyber policy—every state has their own direction and priorities, yet must reconcile these needs with the realities of using a cross-boundary socioeconomic tool such as the Internet.

Panel 3: International Organizations: Updates

- **Mr. Neno Malisevic**, Cyber Security Officer, Organization for Security and Cooperation in Europe
  "The OSCE and Cyber TCBMs: An Update"
- **Mr. Ian McConville**, Deputy Permanent Representative to the Conference on Disarmament, Australian Permanent Mission to the United Nations, Geneva
  "Next Steps for Cyber TCBMs in the ASEAN Regional Forum Context"
- **Mr. Leonard Lu**, Senior Officer, Security Cooperation Division, ASEAN Political Security Department, ASEAN Secretariat
  "The ASEAN's Cyber Confidence Building Measures"

Panel 3, "International Organizations: Updates", brought together representatives of regional organizations to discuss cyber-related developments. The first presenter, Mr. Malisevic of the OSCE, focused on the achievement of the December 2013 OSCE ministerial meeting and resolution which resulted in an initial set of voluntary and non-legally binding TCBMs for OSCE member states. These TCBMs focused on transparency measures allowing for a high degree of information exchange on several levels, specifically exchanging views on national

and international threats; ensuring an open and accessible internet; facilitating cooperation between public and private sectors; protecting critical ICT infrastructure; exchanging best practices, awareness-raising, capacity-building, and lessons learned; coordinating state responses; and the provision of a list of national definitions of relevant terms. As a first round of regional TCBMs, Mr. Malisevic felt they should be seen an expression of goodwill by OSCE member states.

Another organization working towards regional cooperation on cyber issues is the Association of Southeast Asian Nations (ASEAN). In his presentation, Mr. McConville of Australia, an ASEAN member state, explained that because of the enormous global dependency on cyberspace and ICT, cyberattacks are virtually inevitable, therefore the international community should focus on conflict mitigation. For member states of ASEAN, Mr. McConville felt the focus of conflict mitigation dialogue should be who do we call when we have a cyber-related problem? Determining the answer to this question will better prepare regional organizations and states to deal with future cyber issues. For ASEAN, establishing the ASEAN Regional Forum (ARF) in 1993 was a successful first step. The ARF is not treaty based but rather a political grouping and uses a consensus-based decision-making process. It has 27 members, 10 of which belong to ASEAN. The central goals of the ARF are the promotion of dialogue on political and security issues confronting the region and of TCBMs. In this context, ARF has a record of activity on cyber issues going back over a decade beginning with cyber terrorism in 2004.

Mr. McConville cited two recent ARF developments that are important for the continuation of regional cyber TCBMs. The first was a ministerial statement adopted in July 2012 that detailed organization-wide cooperation on ensuring cyber security. The second was a September 2012 seminar on TCBMs that signified the ARF's continued determination to address cyber stability in a regional context. The ARF has also since drafted a second ministerial statement that details a work plan on security and the use of ICTs. The plan, currently in its final stages of development, will involve the creation of an ARF database for cyber threat management, a lessons learned section, and an updatable list of TCBMs for states to share and adopt. Mr. McConville acknowledged that this work plan is ambitious but he argued that even if only some aspects of the plan materialize, it will contribute to a greater understanding of the complexity and risks posed by cyber conflict. He concluded his presentation by explaining the next step for ASEAN: a March 2014 regional cyber TCBMs workshop that will bring together a functioning network of senior policy advisers to help prevent conflict-related miscalculations, escalation, or tension.

The last speaker in the panel, Mr. Lu, contributed a technical overview of ASEAN's history of engagement with cyber TCBMs. He began by describing various relevant ASEAN mechanisms—the ASEAN Senior Officials Meeting on Transnational Crime, the ASEAN Ministerial Meeting on Transnational Crime, the ARF, the ASEAN Telecommunications and IT Ministers Meeting, the ASEAN Telecommunications Regulators Council, the ASEAN Telecommunications Senior Officials Meeting, and the ASEAN Senior Officials Meeting on Social Welfare and Development. Mr. Lu described the trajectory of ASEAN involvement in cyber-related issues, and noted that much of the association's early involvement was related to addressing cybercrime, such as the 2002 Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime. As ICTs have become a concern of national and regional importance, Mr. Lu explained that some ASEAN offices have started to address the issue through initiatives such as the 2005 Framework and Action Plan for Cooperation on Network Security and the 2012 Mactan Cebu Declaration. Mr. Lu also detailed ASEAN work in 2012–2013 on combatting cyber pornography and cyber prostitution in South-East

Asia. All of these functions point to an increased regional concern for cyber stability and the development of concrete TCBMs to combat the multitude of cyber-related issues.

The discussion period following this panel explored which level is the most appropriate for determining the direction for cyber stability initiatives. One participant commented on the importance of cyber agreements at all levels—nationally, bilaterally, regionally, and multilaterally—and argued that the challenge would be figuring how to knit these together to create a global agreement. Another participant explained that discussions at the OSCE regional level were influenced by the 2013 GGE report—the OSCE found the report to be one of the most influential processes in their work. Thus, the global-level discussions informed the regional-level discussions, and it is hoped the 2013 OSCE ministerial agreement can reciprocate and become a model for global agreements.

Panel 4: New Approaches

- **Mr. Ben Baseley-Walker**, Programme Lead, Emerging Security Threats, UNIDIR
  "Addressing Cyber Stability within the United Nations System?"
- **Mr. Jan Neutze**, Director of Cybersecurity Policy, Europe/Middle East/Africa, Microsoft
  "Cyber Stability in Emerging Markets: An Industry Perspective"
- **Amb. (ret.) Daniel Stauffacher**, President, ICT4Peace Foundation
  "Cyber TCBMs: Looking to the Future"

Panel 4 explored the future of the cyber stability conversation and asked how the international community can more comprehensively address it. Non-governmental organization and private sector representation on this panel furthered discussion on how to bring all relevant stakeholders into the conversation. The first presenter, Mr. Baseley-Walker, framed the broad topic of cyber stability and situated it in the international context. Cyber stability is difficult to define in terms of the extent of its reach, he explained, as one cannot simply assume it is a military issue, a technological issue, a national security or an international security-related issue—rather it should be seen as being all of the above. For him, this interrelation between these facets is key to the cyber stability discussion. In the United Nations General Assembly, while there has been continued discussion on ICTs and cyber stability, these discussions have not had a particularly high priority. Involving national, regional, and multilateral perspectives is essential for addressing cyber stability; however a major challenge is that technical developments in the cyber domain move faster than traditional policy-making processes. Given this reality, the key to making progress towards cyber stability is to determine a place for effective discussion of cross-cutting cyber issues within the international system and develop coordination and communication mechanisms for Member States.

It seems clear that the private sector can offer the international community a great deal of experience and expertise when developing such coordination and communication mechanisms. As a representative from Microsoft, Mr. Neutze advocated for further incorporating the private sector in cyber stability conversations, and his presentation explained how this could be mutually beneficial for all stakeholders. By 2020, Mr. Neutze estimated data volumes will be 50 times what they are today and 75 per cent of that data will pass through some form of third party control, most likely a cloud. Thus the need to understand the key factors that contribute to cyber stability is essential. Mr. Neutze argued that the larger and more technical the cyber issue facing a given society, the harder it will be for a government to face the issue without involving the civil/private sector. Historically,

governments have held the role of protector and regulator of the Internet; however they have also shown themselves to be exploiters of that role. In his view, distributing the responsibility for cyber stability can be beneficial for all if there is collective agreement on strengthening defence and limiting offence as a formula for cyber stability. In practice this could involve the private sector (including ICT companies) prioritizing security in their strategies, strengthening cyber defence capabilities, and helping with the processing and storage of data. The government could then strengthen legal protection for Internet customers and support international security arrangements. In the development of these security provisions, Mr. Neutze suggested a "G20+20" model for addressing ICT conflicts and countermeasures at the multilateral level, where the latter "20" would represent major ICT companies in the private sector. This would ensure a variety of opinions from contributors to cyber stability.

In addition to the private sector, the cyber stability conversation could greatly benefit from non-governmental organization input. Amb. Stauffacher of the ICT4Peace Foundation explained his organization's contribution through their work on crisis information management in the use of new information technology. According to ICT4Peace, this work requires a safe and secure Internet. For this reason, and on ICT4Peace's own initiative, the foundation sought to drive cyber stability dialogue forward by participating in the Conference on Cyberspace in Seoul in 2013, which focused on TCBMs and the involvement of industry and civil society. His experience at this seminar further confirmed the need to increase inclusion of all stakeholders in cyber stability discussions.

Another ICT4Peace initiative was the 2013 report on TCBMs titled Confidence Building Measures and International Cyber Security. In this document, the Foundation examined experiences in conventional arms and nuclear disarmament negotiations, compared relevant TCBMs, and explored how they might be applied in the cyber stability context. Concluding his presentation, Amb. Stauffacher suggested that 2014 should be the year to work on developing norms and common understandings in the cyber stability community.

A short discussion period followed this panel. One participant saw the "G20+20" model as a compelling one because it acknowledged that cyber stability is not only the purview of governments. Another inquired about "zero day" vulnerabilities—vulnerabilities in cyber infrastructure that have just been uncovered. Markets exist where, traditionally, actors such as Google and Mozilla buy information pertaining to these vulnerabilities; however, recently governments have been entering this market and driving up prices. Zero-day vulnerabilities are seen as a destabilizing factor for cyber stability with the ability to alter the distribution of power between the civil/private sector and government. Acknowledging that this is a huge concern for the private sector, another participant believed the zero-day vulnerabilities phenomena resembled an unregulated global arms race in cyberspace.

Concluding Remarks

Mr. Baseley-Walker concluded the seminar by thanking the panellists for their contributions and once again reiterated UNIDIR's commitment to supporting the international community in developing policy-relevant thinking, analysis, and facilitative events to work towards an improved climate of stability in the cyber domain over the coming years.

UNIDIR

UNIDIR Cyber Stability Seminar 2014: Preventing Cyber Conflict

UNIDIR held its second Cyber Stability seminar entitled "Preventing Cyber Conflict" on 10 February 2014 in Geneva, Switzerland. The seminar was organized with the support of the governments of Australia, Germany, and Switzerland. The seminar presented an opportunity for states and relevant stakeholders to discuss how to take pragmatic steps towards a more stable and predictable cyber environment. With particular attention paid to the risks of escalation in cyber conflicts, the seminar addressed the growing need to develop mechanisms for discussion, education, and constructive engagement on how to improve cyber stability in the multilateral context.