UNIDIR Cyber Stability Seminar 2015: Regime Coherence

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.

The report was drafted by Suresh Guptara.

www.unidir.org

UNIDIR Cyber Stability Seminar 2015:
Regime Coherence

Seminar Report

9 July 2015, Geneva, Switzerland

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

Introduction

UNIDIR's Cyber Stability Conference Series presents an ongoing opportunity for stakeholders to discuss how to take practical steps towards a more stable and predictable cyber security environment. The 2015 edition of the annual seminar focused on the topic of "Regime Coherence".

The multitude of cyber initiatives at the international, regional and national levels that we see today are both very timely and critically needed. With the increasing level of cyber interest and activity, it is important to consider how current and future norm-setting cyber initiatives can be coordinated to further the development of a pragmatic, global approach to cyber stability. The seminar brought together stakeholders from the Geneva diplomatic community, cyber industry, and policy makers for discussions that explored ways in which the cyber community can better align strategic goals, and promote a stable and secure cyber environment.

While presentations by panellists were on the record, all discussion was held under the Chatham House Rule.

PROCEEDINGS

Welcoming Remarks

- **Mr. Jarmo Sareva**, Director, UNIDIR

Mr. Sareva opened the seminar by noting that the cyber domain is an extension of the existing international security arena and that stability is to be found at the nexus of international and national law, responsible state behaviour and norms. UNIDIR's work on cyber issues is situated at this nexus, and in particular centres on how national law and state behaviour either apply to cyberspace or are being translated to the cyber domain. In this regard, of particular importance is not only consideration of how existing legal frameworks are applied in cyberspace, but also developing shared understandings of such.

The Director pointed out that despite the steady growth of cybercrime and the increasing frequency and complexity of cyber attacks, significant progress is being made in regional and transnational Confidence Building Measures (CBMs), several fora on cyber issues are proving successful, and they are strengthening capacity across the board in the cyber community. Of particular relevance, Mr. Sareva pointed out, is when ICT resources are considered part of an arsenal and hence factored into military and strategic considerations. Such matters must be addressed multilaterally, as averting risks associated with the military aspect of cyber, and understanding how international law applies, is crucial. He called for the international community to ensure multilateral discussions keep pace with technological developments and remain relevant, and highlighted the recent UNIDIR publication *Towards Cyber Stability: A User-Centred Tool for Policymakers*, which offers a vision of how to support policy makers in this process.

Mr. Sareva concluded the opening by reminding participants that Geneva stands to be a hub of international cyber diplomacy, due to its long established role as a centre for multilateral disarmament and security discussions, but also its capacity on other cyber-relevant and global governance topics. Geneva offers a forum for the international community so that the benefits of cyber technologies can be used peacefully by all and to the benefit of all.

Panel 1: UN Machinery: A Strategic Approach to Understanding Cyber?

- **Moderator: Ms. Camino Kavanagh**, Senior Advisor, ICT4Peace
- **Mr. Karsten Geier**, Head, Cyber Policy Coordination Staff, German Federal Foreign Office
  "Cyber as an Emerging Security Challenge: What Are the Next Steps after the UN GGE?"
- **Mr. Tomas Lamanauskas**, Head, Corporate Strategy, International Telecommunications Union (ITU)
  "ITU WSIS Action Line C5, Linking C5, Linking to a Wider Approach"
- **Ms. Ngozi Onodugo**, Consultant, ICT Analysis Section, Division on Technology and Logistics, UNCTAD
  "UNCTAD: Cyber, Development and International Security Impacts"

Ms. Kavanagh opened the first panel by asking whether a strategic approach is possible, considering how difficult it can be to develop strategic approaches even within the UN framework, and especially when civil society, the private sector, and other actors are part of the discussion.

Mr. Geier responded that not only is a strategic approach possible, it is required. However, this does not mean it is easy. Numerous states pursue cyber capabilities, and many give some role to the military. In 2013 UNIDIR published *The Cyber Index: International Security Trends and Realities* which he sees as a benchmark document analysing the publicly available information, and he hopes this blueprint will be taken forward. Cyber capabilities are distinct from traditional weapons of war. Battleships, bombers and cruise missiles are not available for private purposes, but there is a market for malicious cyber capabilities which is accessible to anybody.

Mr. Geier outlined four possible scenarios for the use of cyber capabilities in international conflict:

1. **All-out cyber war**—For the time being this is not a realistic scenario, but rather the domain of science fiction. Thus we should be careful of using the term 'cyber war'.
2. **Limited use of cyber capabilities as part of a larger warfighting effort**—This scenario is realistic as most militaries seek to disrupt or disable others' capabilities, and infrastructure is also a target. We have to expect cyber to be an aspect of any future conflict.
3. **Use of cyber capabilities as an element in hybrid conflicts**—Multi-layered efforts to destabilise a state combine traditional subversive efforts with cyber operations. Cyber capabilities are integral in such conflicts, and are especially useful because an attacker is afforded a significant degree of anonymity.
4. **International military crisis developing from a cyber-action**—In recent years there have been a number of incidents that clearly fall below the threshold of an armed attack. But in the perception of the targeted country, such attacks may reach a threshold where national sovereignty and stability are threatened. That country may then choose to react, which may lead to an escalation of conflict. This scenario of a cyber-incident developing into a physical world crisis is highly worrisome.

As cyber capabilities favour offensive action rather than defensive ones, their use may introduce an element of insecurity into international relations. Diplomats and international security experts must decide how to respond to this destabilisation.

Mr. Geier gave an initial overview of the work of the most recent UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, in which he represented Germany. The GGE maintained that international law applies to the use of Information and Communication Technologies (ICTs) by states, and offered an explanation of the different views on *how* it applies to questions of jurisdiction over ICT infrastructure, state sovereignty, the inherent right of states to take measures consistent with international law as recognized by the UN Charter, the principles of humanity, necessity, proportionality and distinction, the use of proxies, and international obligations regarding internationally wrongful acts.

The GGE also considered the distinction between the binding rules of existing international law and voluntary non-binding norms. The latter are meant as a reflection of the international community's expectations, and could cover measures to increase stability and security in the use of ICTs, how to respond to ICT incidents, the use of state territory for internationally wrongful acts, and cooperation in combating terrorism and criminal activity.

The result of the 2014-2015 GGE (the fourth since 2005) could be taken further in three possible venues: convene another UN GGE, establish an open-ended working group, or take the topic into the Conference on Disarmament (CD). Because of the difficulty in establishing a starting point, reaching consensus and balancing inclusiveness with expert knowledge, Mr. Geier does neither see an open-ended working group, nor the CD as workable. The GGE would work best, although he acknowledges that there are legitimate arguments against another GGE, such as its limited membership.

An additional thought provided by Mr. Geier was to convene an advisory board composed of individuals invited by the Secretary-General from government, civil society, the private sector and academia. This board could produce an annual report on the ICT impact on international peace and security. However, given the importance of the cyber issue, he encouraged everyone to think "outside the box" about constructive ways to build international understandings.

While noting that policy discussions are important, **Mr. Lamanauskas** raised the importance of what happens on a daily basis. The hacking of e-mail accounts, or money stolen from bank accounts are—at the very least—highly inconvenient for individuals, but once amplified by the number of Internet users these daily matters become a security issue. It can often be hard to determine the intent of a given cyber-incident: is it hacktivism, hooliganism, or military in nature. Mr. Lamanauskas argued that managing these daily risks can prepare the way for managing high-level risks. He noted that focusing on high-impact risks alone might overly politicize discussions and cooperation, ultimately inhibiting the capabilities of states to protect their own citizens.

The ITU has an important role to play in ensuring there are no such gaps. By design, the ITU is comprised of not only Member States, but also the private sector and academia, and, through World Summit on Information Security Action Line C5, has the mandate to work together with all parties to build confidence. Because of its wide stakeholder group and by leveraging Public-Private Partnerships (PPPs), the ITU can cover a range of issues including cyber threats, raising awareness, tackling spam, examining privacy issues, data protection, and real time crisis management. In response to this mandate the ITU Secretary General launched in 2007 the "Global Cybersecurity Agenda" with five associated pillars, recognising the dual nature of ITU as a facilitator working with governments and other partners and UN agencies, and as an implementing agency taking action under the mandate of a Member State.

Mr. Lamanauskas raised the point that, while cyber exercises or implementing Computer Emergency Response Teams (CERTs) through the ITU may not be genuine CBMs, through such activities countries learn to collaborate at a technical level, and on this foundation confidence can be built, for example facilitated by UNIDIR and other bodies.

Coordination within the UN is important, especially with the Global Development Agenda review. The Sustainable Development Goals (SDG) cannot contribute to development if we do not have trust. In that context, for the better understanding of Member States, the ITU with others contributes to mapping how the SDGs can also be security specific.

In Mr. Lamanauskas' view, the only way to ensure regime coherence is not to have one single regime or framework, but to understand how different parts of the system are interlinked, so different actors can understand each other and collaborate more effectively with one another.

In international collaboration, **Ms. Onodugo** reminded participants, the network is only as strong as its weakest link, and she therefore raised the need to strengthen the capacity of developing countries. UNCTAD supports developing countries especially in relation to cyber threats impacting e-commerce. Three areas are covered by UNCTAD's Toolbox on Cyber Laws: regional and national capacity building workshops, law revision and preparation of a regional cyber law framework, and a cyber law tracker. The aim of these three areas of work is to raise awareness and develop the skills of policy- and law makers, and to build networks at the regional level to enable collaboration and sharing best practices. Over 2,400 policy- and law makers have been trained through the more than 30 workshops, with the goal that they in turn will train others.

Through its cyber law tracker, UNCTAD is mapping legislation in developing countries and is currently in the process of adding names and links to the specific laws. Ms. Onodugo shared some of the findings so far, including the fact that Africa has the lowest percentage of countries with cybercrime legislation, and that while over 90% of developed countries have cyber laws, transition economies have an even higher percentage. Further findings will soon be available, and a recent study with the Economic Community of West African States (ECOWAS) relating to cyber law harmonisation will be published later this year.

Returning to the idea of the weakest link, Ms. Onodugo said that we must encourage developing countries to enact cybercrime laws. Because of the complexity of cybercrime, no state can address the issue alone, so achieving compatibility between the regional and national level is imperative.

Before opening the floor for discussion, Ms. Kavanagh drew the distinction between the different levels the panellists looked at: the level of states' behaviour and discussions on norms, system security and public safety in response to daily threats, and transnational threats which impact the international security community.

In the discussion period there was agreement that both terrorist uses of ICTs and Human Rights issues were very important, but the GGE had not extensively covered these issues as they were beyond the mandate and the expertise of its members. It was noted that other bodies cover both these issues. One participant pointed out that, at the beginning of the year, China and Russia circulated a renewed International Code of Conduct for Information Security, some of which has been reflected in the GGE, but that perhaps it is time to negotiate acceptable conduct in a systematic manner. A response suggested it was up to the authors to see how the Code of Conduct could be used further, and participants were reminded not to forget the importance of progress on specific topics even if they do not resolve all issues. The legitimacy of the GGE was acknowledged to be open to question, and issues of balancing effective work, expertise, and broad membership were raised. It was strongly advised that, whatever body takes over from the GGE, the mandate should build on the recommendations of the four GGEs so far, as there is a danger that starting anew will unravel the progress made so far. Rather than a new venue, the suggestion of an in-between step was raised, whereby consultations or hearings would reach out to different circles and include regional groups through their representatives, especially considering the vital work of two consultants of the GGE, without whom consensus probably would not have been reached. It was pointed out that the UN General Assembly can mandate UNIDIR to undertake research and other projects which might be a useful and cost-effective step in preparing the way for GGEs, especially considering that each GGE costs the UN Member States upwards of US$ 1 million.

Panel 2: Avoiding Dissonance:
A Round Table on Future Inter-Regional Collaboration

- **Moderator: Ms. Eneken Tikk-Ringas**, Senior Fellow for Cyber Security, International Institute for Strategic Studies (IISS)
- **Ambassador Adam Blackwell**, Secretary for Multidimensional Security, Organization of American States (OAS)
- **Ms. Souhila Amazouz**, Senior Radio Transmission and Broadcasting Officer, Infrastructure and Energy Department, African Union Commission
- **Mr. Ben Hiller**, Cyber Security Officer, OSCE Transnational Threats Department, Organisation for Security and Co-operation in Europe (OSCE)

Ms. Tikk-Ringas started the second panel by raising questions about the current drivers in the debate in different regions, understanding where the different regions and countries are, and where links exist between the UN and regional issues.

Ambassador Blackwell explained that the Organization of American States (OAS) sees cyber in the multidimensional way that Mr. Sareva mentioned at the Seminar's opening, noting that it is not purely a technical issue, but an accelerant of other issues. OAS adopted a comprehensive cyber strategy in 2004. Balancing the needs and requirements is complicated due to the asymmetric capabilities present among OAS Member States, but the OAS has successfully focused on, for example, developing a culture of evidence and collaboration.

Development of a national cyber security strategy is a vital first step, and the OAS has a model which seeks buy-in through different frameworks and roundtables. Columbia is a successful example of this multi-stakeholder buy-in. While legislation is important, it is more important to have an overall national strategy, and develop sub-sectoral strategies within the respective national cyber strategies.

Capacity building and training within the OAS seek to raise awareness of legislators, business and government leaders, for example, through table-top crisis management exercises using a mobile lab. Talks are being held with universities to offer executive-level training courses for key decision makers. Beyond the important work of developing a CERT network to exchange information in real time, the OAS is looking at how to connect to other regional networks.

Further initiatives are directed at users, related to password security for example, or at businesses, for example, ensuring that whitelisting happens, or that server software gets updated. An annual report identifies the state of preparedness of Member States, which helps drive behaviour in the right direction. The OAS maintains a roster of experts and provides, upon request, technical assistance missions to Member States.

The Ambassador concluded by saying that a transformation map would help eliminate overlap and to identify gaps. He noted that some indicators, especially around legislation, need to be changed, as it is difficult to tell which jurisdiction is concerned, and noted that the illicit economy (which is in size comparable to a mid-range G7 country) has a fundamental impact frustrating development and democratic governance and will not "wait" for working groups to form a perfect plan.

Most countries in Africa still face the challenge of setting up their national cyber strategy, **Ms. Amazouz** told the seminar, even as countries increase access to broadband and consider how best to protect citizens and the private sector. The lack of know-how leaves countries vulnerable to cyber terrorism and espionage, and international cooperation needs to be reinforced, including through CBMs. Whilst many countries have proposed legislation, legal frameworks need further development, the level of participation of both the private and the public sector remains low.

Ms. Amazouz spoke of the African Union Convention on Cyber Security and Personal Data Protection, the objective of which was to set up minimum common terminology in relation to cyber security, and develop provisions relating to harmonising cyber legislation. The work was undertaken by African experts in collaboration with international institutions, and has already been validated through regional level workshops. The convention is now open for notification and signature by Member States, although Ms. Amazouz noted that this is itself also a process as it has to take into account domestic signature processes.

The African Union Commission (AUC) continues to provide assistance to countries building national strategies as capacity-building projects are still at an early stage and CERTs are being set up. To combat the threat of cybercrime, the Convention must be implemented and guidelines regarding strategy must be defined, taking into account existing commitments at the sub-regional, regional and international levels.

Mr. Hiller reiterated that ICTs have made offence easier than defence, and that they have been used in recent conflicts. In his view we currently face a very real risk of miscalculations that could lead to tensions and even to conflict. The increasing use of ICTs by non-state actors is one factor influencing this, which has the potential to further erode trust between states. At the same time, on several key policy issues states remain far apart, and the current fragile global strategic environment is testing relations between states even more. He welcomed, however, that the international community has taken note and taken steps to address these issues, most notably through the GGE whose work has offered a roadmap of how to address these questions.

The GGE found CBMs to be a good tool, and in 2013 the OSCE adopted 11 CBMs targeted at policy makers having a say when a state decides what to do when it feels it has been attacked. These CBMs come in three groups.

1. **Enabling states to 'read' postures in cyberspace**—These build understanding of how states perceive different threats, ultimately allowing states to make better judgements.
2. **Timely communication and cooperation**—These include measures to defuse tensions, and a commitment to raise an issue with another state before acting.
3. **Promoting national preparedness and due diligence**—These allow states to be more reliable partners by protecting their own networks reducing footholds for malicious actors.

The OSCE has an incremental approach to confidence building, compared to ASEAN, which can focus on communication, cooperation and stability at the same time, or the OAS which has already reached a very technical level. These approaches work well in those regions but could not be done at the moment within the OSCE, Mr. Hiller stated.

Regional organisations must be allowed to progress at different speeds, yet there needs to be a thread that binds actors together. Mr. Hiller suggested that at the strategic level, regional efforts should strive towards the recommendations of the GGE report, which should serve as a universal reference on how to achieve stability between states. At the practical level, he used the term 'coordinated fragmentation' to allow for institutionalised inter-regional information exchange, as not enough is currently being done to learn from processes happening in parallel in different regions. He also suggested that regular staff-level talks could be highly effective, and raised the idea of an annual academic council to track efforts, seek synergies, and evaluate progress with regional organisations.

Following the presentations, Ms. Tikk-Ringas pointed out how each of the different regions represent different dimensions of coherence and that different approaches enable practical steps to be taken without long task lists that are encumbered by ideological differences.

Starting with the weakest link concept, some participants thought that national cyber security strategies had to be prioritized, disagreeing with starting at an overarching regional strategy. There was general consensus, however, that a national strategy should be in place before domestic legislative issues are tackled.

It was acknowledged that one of the largest challenges is to get through the foreign-ministry 'filter' and speak to interior or ICT ministries, especially as cyber is not just a military domain and must take broader communities into account. This issue is tied in with the question of how to mainstream cyber stability across policy areas and break through silos, given the difficulty of doing so even in other areas and especially within the UN. In terms of identifying overlap and gaps, a positive sign is that there are various mapping initiatives underway.

Panel 3: Cyber and International Law

- **Moderator: Colonel Aapo Cederberg**, Senior Programme Advisor, Emerging Security Challenges Programme, Geneva Centre for Security Policy (GCSP)
- **Ambassador Kriangsak Kittichaisaree**, Ministry of Foreign Affairs, Thailand and Member of the International Law Commission of the UN
  "An Asia Pacific Approach to the Use of Force & Cyber"
- **Ms. Katherine Wanjiru Getao**, ICT Secretary, MoICT, Kenya
  "Emerging Cyber States: Is a Conversation on IHL Relevant?"
- **Mr. Nils Melzer**, Senior Advisor, Division for Security Policy, Directorate of Political Affairs, Federal Department of Foreign Affairs, Switzerland
  "Military Perspectives: Top Legal Issues in Cyber for 2016"
- **Ms. Eneken Tikk-Ringas**, Senior Fellow for Cyber Security, IISS
  "The Quest for New Norms: State Exercise of Normative Power"

Colonel Cederberg raised three questions at the opening of the third panel, the first relating to the line between what is considered use of force and what is a crime, the second asking about the balance between the power of state security services and need for the protection of citizens, and the third concerning the evolving nature of the cyber landscape leaving legislation behind—and what that implies for controlling and supporting the private sector and civil society.

Traditionally, the main concern of the Asia Pacific region, according to **Ambassador Kittichaisaree**, has been cybercrime, as no cyber attacks have yet registered at a scale that could be considered a conflict. However, some States in the region are now shifting their attention from cybercrime to cyber warfare.

For members of the Shanghai Cooperation Organisation (SCO), information warfare is a threat to international peace and security even if there is no kinetic threat. In the Ambassador's view this is a very liberal interpretation of the UN Charter, especially Article 2(4), and the SCO demonstrates a very broad understanding of what constitutes a threat by cyber means.

Three main conclusions have been reached regarding international law in cyberspace.

1. The UN Charter and international law continue to apply to cyberspace.
2. The principle of non-interference remains.
3. Requisite levels of proof regarding state and non-state actions remain unclear.

Based on these conclusions, further discussion is necessary to consider what constitutes an armed attack in the context of cyber, for example. The Ambassador pointed out that the United States government commonly cites some of the following cases as examples of what they would consider use of force: operations that trigger a nuclear power plant meltdown, operations that open a dam above a populated area causing wide-spread disaster, and interference in air traffic control resulting in airplane crashes. However, this does not address the difficult—but not impossible—task of how to find the person or state behind an attack, or determining whether an individual acted as a proxy on behalf of a State. In the case of the Sony hack in November and December 2014, the US Federal Bureau of Investigation attributed the attack to a state, but in the view of the Ambassador the released evidence was only sufficient for a court of public opinion, not a court of law.

The situation becomes more complicated when Article 51 of the UN Charter and states' right to act in self-defence is invoked in response to actions by non-state actors. This is a concept that has not yet been looked at extensively, but the possibility of action against non-state actors cannot be excluded.

In her comments, **Ms. Getao** noted four reasons why International Humanitarian Law (IHL) is relevant for emerging cyber states.

1. **The potential for conflict exists**—There is insecurity due to crime as well as inter-state tension. Inequality exists as know-how and capabilities are distributed unevenly, and with so much money flowing through mobile transactions every day there are clear incentives for criminals.
2. **Effects of an attack become increasingly harmful**—As emerging cyber states transition to new tools they become vulnerable. Ms. Getao provided two examples. One was the 2014 Mpeketoni (Kenya) attacks, where the mobile communication tower was disabled before the physical attack, preventing victims from calling for help. Another was the effect in neighbouring countries of the 2008 post-election violence in Kenya, where critical infrastructure was impacted because of their reliance on Kenya, before resilience had been built up or contingency plans implemented.
3. **Emerging cyber states may be most at risk**—Good infrastructure but lower capacities means there is a higher risk of abuse, and the risk of proxy use. An example given included an incident where some Chinese citizens, operating from Kenyan territory, targeted Chinese banks. Ms. Getao stressed that China was the victim and was able to assist the Kenyan authorities, but raised the question of what would have happened had China considered the action a state-endorsed attack. Similarly, there is the risk of proxies, whose capabilities far surpass those within the small national cyber security expertise pool.
4. **IHL impacts emerging cyber states**—With the increasing presence of non-state actors including contractors, corporations and terrorists, as well as new weapons and technologies, IHL has an important role to play in informing the variety of discussions being held.

Ms. Getao further pointed out that while cybercrime legislation and IHL cover times of peace and times of armed conflict respectively, in times of "less than armed conflict" it is unclear which domain is relevant. Important questions that need to be addressed include how big the gap is, what happens post-conflict, and how risk analysis can take into account geopolitical, economic, technological and socio-cultural factors.

The military, **Dr. Melzer** said, still has the traditional roles of offensive, defensive and stabilisation capabilities, and depending on domestic legal settings these can be broadened to include collaboration with law-enforcement agencies and performing peace-time intelligence operations. These roles do not change when it comes to cyber, although the specifics might. Dr. Melzer endorsed earlier comments concerning the consensus that international law applies in cyberspace, and added that this is something the Swiss government fully supports. The question, however, is how it applies, and in his view the problems cannot necessarily be solved by law or by lawyers alone.

For example, Dr. Melzer explained that the legal framework of attribution is well developed, but the challenge is to find the facts. He compared the current state of cyber identification to aircraft identification during the Second World War and the development of radar. Similarly, institutional challenges also exist outside the cyber realm, for example, when global corporate partnerships make it difficult to understand which laws apply where.

As for the issue of the scale of a cyber attack that would justify self-defence, this again is not limited to cyber, as there exist other types of operations that fall below the level of armed conflict. The problem of armed non-state actors and actors we cannot identify exists in the cyber domain as well as in traditional theatres. The distinction between combatants and civilians is more difficult in cyberspace, but this again is also problematic in kinetic conflicts.

One contemporary legal issue Dr. Melzer mentioned was whether civilian data constitutes a civilian object, in which case it cannot be attacked. The problem he sees with this discussion as a whole is that it is overly specific, referring to Charter language drafted at a time when there were only persons and physical objects. Rather than sticking to the specific words that were used at the time of the drafting of particular treaties, we should look at the spirit behind them. Certain issues may need new laws, but we should interpret existing legislation and see where states need to clarify their definitions, and then see where the gaps are.

In her comments, **Ms. Tikk-Ringas** added another layer of complexity to the discussion. Different lawyers and different countries understand and teach law differently, and therefore, their interpretation of law is shaped by their ideas, values and backgrounds. For this reason differing views on the binding nature of the articles on state responsibility or differing interpretations on what constitutes an armed attack, for example, are far from being a random confusion, but they represent differing state views and different nuances in interpretation. Each of these questions still constitutes a complex and complicated matter that needs to be addressed by all governments, the private sector and civil society.

In her view, the main value of the conclusions of the recent GGE were two-fold. First, it is an affirmation that states are bound by existing international law. Even though differences may arise in interpretation, existing law is at least taken as a starting point for further developments. Secondly, there is an invitation to have an open exchange of views, which is important when one thinks of power in the context of norms, because, for some states, the absence of clarity provides a convenient space for manoeuvre.

Some members of the international community are wrestling to frame the conversation, others are demanding inclusion. There is not yet agreement on the best venue to address cyber security questions. This situation is not unique to cyber. Similar dynamics have played out in nuclear issues and space.

The most influential views thus far have come from the US, China and Russia, but we have also seen some countries starting initiatives such as Brazil with NetMundial. For her this signals that a range of states are cognizant of the profound implications on the quality of life and security at the global level.

Conversations about norms are about shaping perceptions of what is permitted and what is prohibited, what is preferred and what is not. It is about permitting one's own interests and those of allies while rejecting others. It is not just about who is at the table, but also about who shares ideas. That said, it is necessary to bring other views to the table, as there are still too few perspectives represented. Otherwise we risk allowing a few strategic decision makers shape the perception of what is acceptable for everyone.

Following the panel, one of the first questions was on when we could expect the first case on cyber in the International Court of Justice. It was felt that while this would be a very significant moment, the legal implications would depend largely on the exact question asked. Further discussion noted that not all legal frameworks are translatable to cyber, for example the concept of 'hot pursuit', and while the UN Convention on the Law of the Sea is an interesting parallel, there are no zoning laws in cyberspace due to its ethereal nature. This led to the question of whether "cyberspace" actually exists: it certainly does in our minds, but physical cables do not constitute cyberspace, although there is no doubt cyber exists as a political agenda.

States must not allow their territory to be used to launch an attack against another state, and Command Responsibility means there is a possibility of being liable because of the requirement for due diligence. In this context, some participants voiced the recognition that state responsibility is a tricky issue but due diligence is certainly important. The vast majority of cases we see where cyber capabilities are used fall clearly below the threshold of armed conflict, yet in some instances these may be internationally wrongful acts. A state of necessity might also come in to play, it was pointed out, which in international law allows states to commit otherwise unlawful acts in order to mitigate 'grave and imminent peril', although it was recognised that a distinction must be made between response to a threat and counter-measures directed against the perceived author of a threat.

Panel 4: New Approaches to Cyber Stability

- **Moderator: Mr. Jovan Kurbalija**, Director, DiploFoundation & Head, Geneva Internet Platform
- **Mr. Nemanja (Neno) Malisevic**, Senior Security Strategist, Global Security Strategy and Diplomacy Team (GSSD), Trustworthy Computing (TWC), Microsoft
  "Transnational Industry Perspectives: What is Needed at the Multilateral Policy for Business Continuity in 2020"
- **Mr. Rutger van Marissing**, Policy Officer, Task Force Cyber, Ministry of Foreign Affairs, Netherlands
  "Capacity Building in the Cyber Stability Field"
- **Mr. Andrii Paziuk**, Postdoctoral Fellow, Institute of International Relations, Taras Shevchenko National University
  "Applying the R2P Doctrine to the Cyber Domain"
- **Ambassador (RET) Daniel Stauffacher**, ICT4Peace
  "The Future of Cyber Stability: A Civil Society Perspective"

In his remarks, **Mr. Malisevic** stated that co-operation is needed, particularly Public-Private-Partnerships (PPPs), as are predictability and stability. CBMs are considered a prerequisite for building much needed norms for responsible state behaviour. But as many stakeholders as possible need to be brought together, including academia and the private sector.

Mr. Malisevic distinguished between two forms of cyber security threats. One form of threat is through opportunistic cyber criminals, who target indiscriminately in order to gain any results. The other type of threats he named were Advanced Persistent Threats (APT), although these are often not advanced but very persistent, and increasingly seek data destruction rather than extraction. This has led to greater international insecurity and legal pressure, which puts innovation at risk. The best way to tackle such threats is through establishing norms.

Governments have a complex relationship with the Internet as they simultaneously use ICTs, to protect the infrastructure and protect citizens, and are exploiters of the Internet. But offensive cyber actions might result in unintended consequences, spill over to affect critical infrastructure, or the global economy. In addition to this, because of the concerns about unintended consequences, cyber insecurity at the global level undermines trust.

In December 2014 Microsoft published a white paper representing a start on proposed norms:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
2. States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
3. States should exercise restraint in developing cyber weapons and should ensure that those which are developed are limited, precise, and not reusable.
4. States should commit to non-proliferation activities related to cyber weapons.
5. States should limit their engagement in offensive cyber operations to avoid creating a mass event.
6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

These starting points on state norms were supplemented with norms for the private sector:

1. Reduce attack services and harden systems, and provide rigorous tools and training.
2. Coordinate vulnerability disclosure.
3. Limit the impact of attacks by working out how to counter proliferation of cyber weapons and their impact.
4. Respond to and recover from attacks on products as soon as possible.

In addition there are two roles the private sector can play, by providing expertise on norms and contributing to the process. The collaboration should be a two-way endeavour, where states should invite the private sector, but when invited, the private sector must contribute to the entire ecosystem not just their own bottom line.

Mr. van Marissing noted that cyber operations are increasingly a tool for power projection, with advanced capabilities growing rapidly and leading to instability. While it is legitimate for countries to improve their cyber defence capacities, he acknowledged that there is a risk of being caught in a classic security dilemma where defensive moves are perceived as threatening by others. He pointed out that often the technical people are less interested in these political questions when concerned with security measures, but this is a short-term attitude that can only lead to more instability.

One way to address these issues is to build more diplomatic and legal capacity to deal with the challenges. Diplomats can have a moderating effect on technology producers and the hard powers of a state, and should explain that cyber is covered by international law, but they can also lay the important building blocks for long-term security.

In spite of its importance, talking about cyber security alone does not necessarily lead to greater cyber security, Mr. van Marissing cautioned. The international community can get ahead before a problem develops and should acknowledge that cyber stability is a topic for diplomatic engagement in its own right. Building on the basic framework provided by the recent GGE process, we should now turn to implementation and clarification, and work across the spectrum on norms, CBMs and international law so that the GGE report can be translated into action.

Mr. van Marissing explained that the Netherlands believes that regional approaches are appropriate as they provide a bridge between high-level agreements and regional and country specific challenges. The Netherlands has contributed by convening a global conference on cyberspace in April of this year, which saw more stakeholders and states attend than any before in this series. The Netherlands, with its commitment to The Hague as the global centre for law and justice, fundamentally believes in the international legal order and Mr. van Marissing provided two examples of supporting legal work. The first was the recent UNIDIR project with regional meetings on the applicability of international law. The second was the drafting of the second Tallinn Manual, which despite being an academic document and not legal one, he sees as a helpful tool to inform the debate.

Building on the GGE as a basis for a normative framework, recognising cyber stability as a diplomatic problem in its own right, and broadening the discussion, are essential in establishing cyber stability. Mr. van Marissing also gave a loose definition of cyber stability, saying it is a situation where there is sufficient diplomatic capacity and normative understanding so that when a crisis happens, it will at least be known afterwards what should have been done.

The Right to Protect doctrine (R2P), **Mr. Paziuk** told participants, is an obligation of states towards their own population and all populations, and consists of three pillars.

1. The state has the prime responsibility for protecting population from genocide, war crimes, crimes against humanity and ethnic cleansing.
2. The wider international community has a responsibility to assist and encourage states in fulfilling this responsibility.
3. When a state is manifestly failing to protect its populations the international community must be prepared to take appropriate collective action in accordance with the UN Charter.

R2P is applicable regardless of the tools used to commit any of these for mass atrocity crimes and also applies when ICT or the cyber domain is used to prepare and commit them, argued Mr. Paziuk.

ICT is used for prevention, for peacekeeping including early warning, and for disaster mitigation and relief operations. Especially in the case of the latter, regulatory barriers should be reduced or removed, such as licensing requirements to send specific radio frequencies. Mr. Paziuk also stated that the provision of ICTs should be recognised as a form of aid in itself.

Ambassador Stauffacher explained that, while ICTs have been a force for good in many circumstances, they have also been detrimental to peace and security. We currently face an erosion of trust between states, but also between citizens. Civil society and the private sector should be more involved in the discussion of norms and principles, as their participation to date has been minimal. Their participation is not necessarily about decision making, but rather about decision shaping and being part of the process of discussing norms.

The Ambassador saw three practical ways in which civil society can engage.

1. **Transparency and accountability**—There is little information available in the public domain on international, regional and bilateral processes relating to cyber security, and what is available has often received limited scrutiny. Civil society could demand information and monitor discussions.
2. **Participation**—There is a concern for non-public aspects of legitimate national security concerns, but governments have taken concrete steps to include civil society.
3. **Deepening the knowledge-base**—Ideas should first be explored in a non-negotiation space, and the Ambassador highlighted the work of the Swiss government producing a report on CBMs.

Track 1.5 consultations in this field should continue to ensure that there are continual links between different policy areas, security, governance and the private sector, and he noted that capacity-building programmes have been useful.

Following the presentations the question of participation was looked at in more detail. Some participants wondered whether adding civil society and others' views would complicate matters further, while one participant pointed out that it can be difficult to find the right point of contact from the private sector—especially since governments are not necessarily interested in a sales pitch.

In this context a number of voices distinguished between being part of a process which shapes the discussion, and being at the table when a decision has to be made. Those who have knowledge and can contribute to the discussion will remain part of the discussion. It was clear from the discussions that more cross-disciplinary interaction is crucial for cyber security and stability.

One participant worried that without minimum knowledge there cannot be sufficient engagement, and when approached by another government there is a lack of institutions to respond to the request. It was pointed out that UNIDIR recently completed a project on middle powers in outer space, and a question was asked about the applicability of the study of the roles of middle powers in cyberspace. A response stated that since small and middle powers have fewer other means of leverage they have a greater interest in building systems of laws, and have an important role to play in pushing forward thinking on developing normative frameworks.

Concluding Remarks

Wrapping up the seminar, Mr. Sareva emphasized that UNIDIR will continue its long engagement on cyber issues. This is an area where multiple voices need to be heard, including those of the private sector and civil society stakeholders, and UNIDIR intends to continue to leverage its mandate and convening power to organise such interactions, as well as produce different types of practical outputs and activities, examples of which had been mentioned throughout the day.

He thanked the governments of Australia, the Netherlands and Switzerland for their support for the event, as well as everyone for participating, especially the panellists and moderators, and UNIDIR staff for their contribution to the organization of a successful seminar. Mr. Sareva looked forward to welcoming participants back at the 2016 Cyber Stability Conference.

UNIDIR

UNIDIR Cyber Stability Seminar 2015: Regime Coherence

UNIDIR's Cyber Stability Conference Series presents an ongoing opportunity for stakeholders to discuss how to take practical steps towards a more stable and predictable cyber security environment. The 2015 edition of the annual seminar focused on the topic of "Regime Coherence".

The multitude of cyber initiatives at the international, regional and national levels that we see today are both very timely and critically needed. With the increasing level of cyber interest and activity, it is important to consider how current and future norm-setting cyber initiatives can be coordinated to further the development of a pragmatic, global approach to cyber stability. The seminar brought together stakeholders from the Geneva diplomatic community, cyber industry, and policy makers for discussions that explored ways in which the cyber community can better align strategic goals, and promote a stable and secure cyber environment.