UNIDIR

International Law and State Behaviour in Cyberspace Series

Compendium of Regional Seminars

UNIDIR RESOURCES

Acknowledgements

UNIDIR would like to thank the Governments of Germany, the Netherlands and Switzerland for their financial support for the project.

In addition, UNIDIR would like to thank the Governments of the Republic of Kenya, the Republic of Korea, the Sultanate of Oman and the International Telecommunication Union (ITU)—Arab Regional Cybersecurity Center (ARCC) for their in-kind contributions and support of the project.

The meeting reports were drafted by Daniel Golston (Asia–Pacific), Ralf Gutmann and Elena Finckh (Eurasia), and Aïcha Bachir (Africa).

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

* * * * *

Table of Contents

Introduction

With increasing societal reliance on cyberspace comes the need for clarity on how existing international legal instruments and norms apply in this borderless and dynamic environment. Nowhere is this more important than in matters of cybersecurity. Building on the conviction that international law does apply, the question remains: how can it be applied?

The report of the 2012–2013 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE on ICTs) noted the applicability of international law in cyberspace, setting important precedents for norms and other cooperative measures that will shape future discussion of cybersecurity. In the light of the GGE report, and the convening of the fourth GGE on ICTs in 2014–2015, UNIDIR's International Law and State Behavior in Cyberspace Meeting Series project set out to raise awareness and encourage regional dialogue on international law in cyberspace in the context of international security.

UNIDIR carried out a series of regional meetings to provide a forum for states to clarify national positions and regional perspectives on the relevance of different bodies of international law to the cyber domain. In particular, the meetings aimed to engage developing and "middle power" states whose national perspectives are not yet widely expressed in multilateral fora.

The three regional seminars brought together both policy and legal practitioners to explore the cyber domain's legal context as it relates to the Asia–Pacific, Africa and Eurasia regions. The first meeting for the Asia–Pacific region, held in December 2014 in Seoul, Republic of Korea, hosted 50 participants from 22 delegations and 15 states. The second seminar was held in March 2015 in Nairobi, Kenya, with 40 participants from 29 delegations and 17 states from the African region. The third seminar for countries in the Eurasia region took place on 3-4 June 2015 in the Sultanate of Oman. The event was attended by 31 participants from 17 delegations and 14 states.

A key aim for the regional meetings was to encourage exploration of the issues most relevant to the states of each specific region. This generated discussions on regional perspectives and differences, thereby increasing understanding among neighboring countries. Furthermore, the seminars sought to contextualize the cyber conversation in the broader international setting, helping illuminate the far-reaching regional impacts of cyber insecurity or instability . In addition to promoting greater understanding of views within the region, it also provided participants with a network of regional contacts, which in the long term will allow for better communication, coordination and cooperation.

The seminars also focused on **mapping the legal landscape**, addressing some of the major topics and questions in the application of international law in the cyber environment.

The 2013 UN GGE on ICTs noted that international law, particularly the Charter of the United Nations, applies in cyberspace. The goal of cyber stability, benefiting all nations, requires that common understandings of how critical concepts and principles, such as state sovereignty, state responsibility, principles of due diligence, as well as thresholds for international humanitarian law (IHL) and the right to self-defense, apply in this environment.

The seminars also addressed **cyber concepts**, examining some of the legal and political terminology frequently employed in international fora and processes relating to the cyber domain. It was noted that many terms are taken from more conventional legal contexts and are then modified and applied to cyberspace—including terms such as cyber sovereignty, cyber boundaries, and attribution in cyber activities. Establishing common understanding of these terms is essential for the development of a cyber legal regime that is sound, comprehensive, and acceptable to all states.

Another critical issue discussed in all three seminars related to **the use of force in cyberspace** and its legal and practical dimensions. Panelists presented and discussed the legal underpinnings of the use of force in cyberspace and interpretations of definitions and principles under international law, as well as ways in which cyber warfare can be understood through the lens of International Humanitarian Law.

Last but not least, the regional seminars explored **national approaches to and perspectives on cyber stability**, through the lens of national policies and safety measures. Widely sharing national approaches and lessons learned can help animate international cybersecurity discussions, facilitate consensus building on key issues, and enhance cyber stability.

The general sentiment among seminar participants across all three regions was that, in addition to clarity as to how to apply international law tenets and principles to the cyber environment, there is also the need for increased international cooperation and legal assistance in the cyber domain. In this regard, moving forward States will have the opportunity to build upon the specific recommendations on CBMs, international cooperation and capacity building included in the report[1] of the 2015 GGE on ICTs.

UNIDIR's regional seminars were a step forward in building common understandings on the application of international law in cyberspace. However, much work remains to be done. There is a growing recognition that all States have a stake in cyber stability and therefore they must actively participate in these discussions—in order to help shape these understandings and contribute to greater stability in the cyber environment. UNIDIR will continue to leverage its unique mandate and convening power to support this important endeavor.

1 UN document A/70 174.

International Law and State Behaviour in Cyberspace Series

Asia–Pacific Regional Seminar

Conference Report

9–10 December 2014, Seoul, Republic of Korea

Introduction

As part of its International Law and State Behaviour Series, UNIDIR carried out its Asia–Pacific Regional Seminar on 9–10 December 2014 in Seoul, Republic of Korea.

Over the past two decades, there has been a growing reliance on cyberspace applications across a broad spectrum of activities and processes. With this increasing societal reliance on cyberspace comes the need to determine how existing international legal instruments and norms apply in the borderless and dynamic world of cyberspace. As academia and government explore these issues, there is a consensus that international law does apply; however the question remains: in what ways does it apply? In light of the 2012–2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE on ICT) report—which noted the applicability of international law—and the convening of the fourth GGE on ICT, it is an opportune time to explore this question and related conversations.

In pursuit of this, the seminar brought together both legal and policy voices to explore the cyber domain's legal context as it relates to the Asia–Pacific region. Relevant stakeholders were given the opportunity to engage in a dialogue on the complexities and various interpretations of the applicability of international law in cyberspace. This not only promoted greater regional understanding, but also aimed to provide participants with a network of contacts throughout the region that in the long term might allow for better coordination and communication.

PROCEEDINGS

Conference Chair

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

Welcoming Remarks

- **Mr. Yoo Dae-Jong**, Director General, International Organizations Bureau, Republic of Korea

Opening Remarks

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

Mr. Yoo Dae-Jong opened the seminar by extending to all participants a warm welcome from the Republic of Korea. As a state with first-hand experience of large-scale cyberattacks (most recently in 2009, 2011, and 2013), the Republic of Korea takes the cybersecurity conversation very seriously. It has shown a commitment to international progress on the subject by hosting the 2013 Global Conference on Cyberspace in addition to extensive involvement in capacity-building and regional/international cooperation on key issues in the cyber domain.

Understanding both the benefits of and threats from the cyber domain, the Republic of Korea has taken a leading role in pursuing the establishment of international norms and principles for responsible state behaviour in cyberspace. Mr. Yoo noted that in the absence of a commonly agreed upon set of norms and principles in the international community, it is essential to build confidence among states to limit the risk of conflict due to misattribution, misunderstanding, miscalculation, and a lack of escalation controls.

The Organization for Security and Co-operation in Europe's (OSCE) 2013 establishment of a set of voluntary regional norms for state behaviour in cyberspace is seen as an important step for regional cooperation and collaboration on cybersecurity, and Mr. Yoo noted that the Association of Southeast Asian Nations' (ASEAN) Regional Forum (ARF) is also working on a similar set of regional norms. He affirmed that the government of the Republic of Korea supports this regional approach and will continue to engage stakeholders in the cybersecurity discussion not only from the Asia–Pacific region but from around the world.

In Mr. Baseley-Walker's opening remarks, he underlined that the Internet and information and communications technologies (ICTs) are rapidly advancing and our dependence on them, from the daily lives of citizens to government activities, is ever increasing. In tandem with this growth in dependence is a greater vulnerability to malicious cyber activity, which requires the swift production of national, regional, and multilateral policies and initiatives in response. However, policy development can easily take months if not years while rapidly evolving situations require decisions to be made in far shorter time frames—and by all states, not simply the "cyber powers".

UNIDIR's International Law and State Behaviour in Cyberspace Series seeks to spark pragmatic dialogue on the applicability and development of international law in the cyber domain in the most beneficial direction for maximal stability and security. By holding seminars in four global regions (the Asia–Pacific, Africa, the Americas, and Eurasia) the series will provide a platform for regional discussion, and development of regional perspectives

and approaches. Mr. Baseley-Walker sees great benefit in expanding the number of voices in the multilateral cyber conversation—as every state has a stake in a stable and secure cyber domain—and views this seminar as an important contribution to that end.

Mr. Baseley-Walker views cyber policy and law as fundamentally linked—as the international community develops new political and policy approaches, this shapes the legal climate in which states and stakeholders operate. As such, this seminar series was designed to include both policy and legal national representation, as well as civil society. He concluded that increasing interaction among these communities is essential in moving forward the cybersecurity and stability conversations.

Panel 1. Introductory Context

- **Cyber Relevance to the Asia–Pacific Region**
  Mr. Pratap Parameswaran, Director, Political and Security Directorate, ASEAN Secretariat
- **Putting Cyber Issues in an International Policy Context**
  Mr. Fu Cong, Coordinator for Cyber Affairs, Ministry of Foreign Affairs, People's Republic of China

A key aim for this seminar was to encourage an exploration of issues most relevant to Asia–Pacific states and allow for regional perspectives and differences to be discussed, thereby increasing understanding among neighbouring states. Furthermore, it sought to link the cyber conversation with the international policy climate, helping illuminate the far-reaching impacts of cyber insecurity or instability in other realms of international relations. Panel 1 laid out the foundations for such discussions by expanding on the importance of cyberspace to the region and the international policy context.

Mr. Parameswaran opened his presentation by commending the Asia–Pacific region on the leadership it has shown in pursuing dialogue and working towards ensuring a safe, stable, and secure cyber environment. Across ASEAN member states, there are 198,000,000 Internet users, with this figure set to increase as ICT infrastructure advances and becomes more accessible. However, with greater connectivity comes higher susceptibility to cyber-related threats.

Mr. Parameswaran noted that governments are very much aware of this issue, and particularly within ASEAN more attention and resources are being devoted to combating cybercrime. From 2011 to 2013, the prevailing types of cybercrime were telecommunications fraud, hacking, defacing, identify theft, and email/credit card fraud. Combating these issues is a challenge in the ASEAN context due to varying levels of technological advancement and knowledge, and national-level law enforcement capabilities in ASEAN member states. Mr. Parameswaran commended all states that have established Computer Emergency Response Teams (CERTs) and noted that some states have established national authorities on cybersecurity. However, he felt there is much still to be done.

As a way forward, Mr. Parameswaran highlighted several areas for improvement: more concerted efforts to raise public awareness of cybercrime; establishment of public–private partnerships nationally and throughout the region; increased cooperation between relevant agencies and the police in gathering evidence on cases of cybercrime; promotion of regular meetings and dialogue among ASEAN member states on cybercrime; and provision of

opportunities for national-level law enforcement officers to learn about ICTs and enhancing international networking and resources.

Mr. Fu began his presentation by framing cybersecurity as both a developmental issue and a security issue—its ability to contribute to the economic and social wellbeing of humankind means that the cyber domain is a key facet of global human development. Cybersecurity is therefore an integral part of global governance which requires participation from all states, as a cybersecurity deficiency in one state could easily impact others.

In the realm of cyber warfare, Mr. Fu affirmed that the international community should not allow the cyber domain to become an arena of conflict. He explained that many states are developing cyberweapons and establishing cyber military commands. It is the responsibility of the international community, according to Mr. Fu, to never discount the danger of cyber conflict leading to events that destabilize international peace and security. On the issue of cyber terrorism, he noted that cybersecurity has become a priority in counterterrorism efforts as terrorist groups can use the Internet for the dissemination of extremist ideas, recruitment, fundraising, and the organization of activities. While not yet witnessed on a large scale, he warned of the looming danger that terrorist groups may use the Internet to launch direct attacks. He felt that further exploration was required to determine concrete measures for pragmatic cooperation on this issue.

In light of these various dangers and opportunities in the cyber domain, Mr. Fu laid out a series of recommendations for the advancement of coordinated international efforts. These included the pursuit of a new concept of cybersecurity based on common and comprehensive understanding of the current climate and global equities, whereby states and stakeholders would engage in forward-looking discussion based on a mutual respect for each other's security; continued efforts to advocate for and observe the basic norms governing international relations including the principle of state sovereignty, non-interference, refraining from the use of force, and the peaceful settlement of disputes; continued efforts to strengthen relevant mechanisms, such as the ARF and Shanghai Cooperation Organization, for constructing a framework for cybersecurity in the Asia–Pacific; a recognition that security and development are of equal importance in the cybersecurity conversation; and that capacity-building is a top priority moving forward. Mr. Fu concluded his presentation by adding that the People's Republic of China stands ready to engage in full cooperation with all states in the cybersecurity conversation.

The discussion period of Panel 1 focused on the Convention on Cybercrime, a landmark international treaty that seeks to address crimes committed via the Internet and computer networks. It focuses on harmonizing national legislation against relevant crimes and increasing international cooperation. One participant noted that the Convention was drafted by European states and so, while it enjoys widespread European support and the support of a few other states, it may not reflect the international community's stance, or perspectives, on cybercrime. That the Convention gives the right of a signatory state to conduct a transborder investigation without the approval of the state in which the investigation is conducted is seen by some as a major flaw that is not amenable to many states' legal systems. One participant highlighted this issue as one that the international community will face with the "internationalization" of such initiatives; the question of how to extrapolate mutually acceptable agreement from the regional level to the multilateral level is a key challenge in the cybersecurity conversation.

Panel 2. The Legal Landscape

- **International Law and Cyber 101**
  Dr. Marten Zwanenburg, Legal Counsel, Ministry of Foreign Affairs, The Netherlands
- **Proposed Legal and Policy Initiatives in the Cyber Domain**
  Mr. Lee Chul, Director, International Security Division, Ministry of Foreign Affairs, Republic of Korea
- **The Current Cyber Legal Regime**
  Dr. Li Juqian, Professor, International Law School, The People's Republic of China, University of Political Science and Law

Panel 2 tackled some of the major topics and questions raised by legal experts and states in the application of international law in the dynamic and borderless cyber environment. The 2013 GGE on ICT recommended that international law, particularly the Charter of the United Nations, should apply in cyberspace,[2] however this becomes ever more challenging in practice as it must reconcile traditional international legal concepts such a state sovereignty, state responsibility, principles of due diligence, as well as thresholds for international humanitarian law (IHL) and the right to self-defence.

Dr. Zwanenburg began his presentation by remarking that the 2013 GGE on ICT's recommendation that international law is applicable in cyberspace provides a solid foundation for further discussion on the specifics of an international legal regime in cyberspace. In the historic development of international legal regimes, determining state practice has been an important part. However, in cyberspace state practice is not always clear—few states have published statements or strategies on their interpretation of international law in cyberspace or how it applies to government-wide cyber activities. This reality means that reaching international understanding, let alone consensus, on how international law applies in cyberspace is all the more challenging.

To explore some basic notions of international law and how they may apply in cyberspace, Dr. Zwanenburg discussed state sovereignty and state responsibility. While difficult to define, state sovereignty emphasizes a state's independence from other states and an ability to exercise control within its borders. When applied to the cyber domain, which is transborder by nature, questions arise over these fundamental tenets that define sovereignty. Dr. Zwanenburg questioned how the international community could determine state sovereignty in the cyber realm when it is a challenge to determine where specific data resides at any given moment. Furthermore, sovereignty carries with it responsibilities such as the obligation to not knowingly allow one's territory to be used for activities contrary to the rights of other states—a due-diligence obligation. If a state does not have the capacity to know what is happening inside their country as regards cyber activities, to what extent does this due-diligence obligation apply?

The second notion was state responsibility, which Dr. Zwanenburg sees as the idea that a state is responsible for its internationally wrongful acts. He listed two requirements for invoking state responsibility under international law: (1) a breach of an international obligation incumbent on a state, and (2) that said breach is attributable to the state. The second requirement is where he predicted the most difficulty when applied in cyberspace.

2 General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/68/98, 24 June 2013, para. 19.

Determining standards for legal attribution of cyber activities to a state is a massive hurdle as potentially such activities are not carried out by states but by private individuals. The question becomes when is the conduct of a private individual attributable to a state, and what should the standard be?

As Dr. Zwanenburg illustrated, attempting to parse the specifics of international law and apply them in cyberspace can raise more questions than answers. However, he felt that these questions can be answered through international dialogue and work towards consensus through forums such as this Asia–Pacific regional seminar.

In the next presentation, Mr. Lee provided an overview of the various moving parts in international conversations on cybersecurity. He divided his presentation into four sections: the work of the GGE on ICT, initiatives on cybercrime, progress on confidence-building measures (CBMs), and Internet governance.

Moving forward from the oft-cited 2013 GGE on ICT report, Mr. Lee saw that one of the current tasks of the GGE on ICT will be to identify the specific norms and principles that can be applied to state behaviour in cyberspace under current international law. He noted that the Republic of Korea believes that additional norms can be developed over time.

As regards combating international cybercrime, Mr. Lee saw the Convention on Cybercrime as a significant achievement, specifically in its call for harmonized national-level legislation and cooperation among states. However, the fact that the current 47 signatories are primarily Council of Europe member states does pose a challenge, as it is critical that global conventions on cybercrime enjoy widespread participation. Another proposed initiative is an International Code of Conduct on Information Security, which has been put forward by the Russian Federation and the People's Republic of China; however, he noted that this initiative shows little progress due to objections from certain states. His preferred option is a global treaty on cybercrime that calls for the harmonization of national-level legal systems and active cooperation of all states to address cybercrime.

Mr. Lee emphasized the importance of building confidence among states to reduce the risk of misperception and miscalculation. He underlined that the Republic of Korea welcomes efforts to develop CBMs at all levels of governance, and commended many states on establishing bilateral relationships and pursuing CBMs. Regionally, Mr. Lee mentioned the OSCE's 2013 set of voluntary norms for state behaviour in cyberspace, and a second set due to be adopted in 2015, as key steps forward for the region. In the Asia–Pacific, the ARF's Work Plan on Cyber Security is a promising initiative that includes various CBMs; while it is yet to be formally adopted, Mr. Lee felt it is only a matter of time until the initiative has widespread subscription.

On matters of Internet governance, particularly how to distribute and manage Internet resources and related technical standards, Mr. Lee saw two distinct groupings of states: those in support of a multi-stakeholder approach (including states, technical experts, industry, academia, and civil society), and those in support of a government-centric approach, with assistance from the International Telecommunication Union (ITU) and other international organizations. He commented that in principle the Republic of Korea supports the multi-stakeholder approach, with the caveat that one needs to consider that, in some aspects, government should bear more responsibility than any other stakeholder.

As the final presenter on this panel, Dr. Li provided participants with a review of the current cyber legal regime. In his view, current international law does provide a general framework

for governing activity in cyberspace; however, specific rules are needed for the idiosyncratic nature of the cyber domain. In addition, he noted that any future cyber-specific international law should be capable of coexisting with national law.

Dr. Li stressed the centrality of the Charter of the United Nations and the fact that it provides the basic legal parameters for cyber activities. He felt that all cyber *lex specialis* must be in compliance with the tenets of the Charter, to which all United Nations Member States have committed themselves. In addition to the Charter, he saw several key sources of law that can be applied to cyber activities, as codified in the Statute of the International Court of Justice: (1) existing international treaties: although there are not specific cyber treaties in place, legal instruments do exist that may be applicable to cyber activities; (2) international custom: while there is no specific customary international law related to cybersecurity, he sees the development and implementation of customary law in other fields as a possible reference for the cyber domain; and (3) the use of general principles of law: he sees many principles that could contribute to a legal regime. Additionally, Dr. Li sees the value of subsidiary sources, that is "judicial decisions and the teachings of highly qualified publicists"[3], and feels they are relevant to the cyber domain. In addition to these sources of law, Dr. Li stressed the importance of several key legal principles that must be upheld when developing cyber legal tools, the two *jus cogens* principles of state sovereignty and the lawful use of force. As regards jurisdiction of a state, Dr. Li noted the relevance of the territorial (activities taking place within the borders of state) and nationality principles (nationals of a given state).

For Dr. Li, while there may be a tentative basis for an international cyber legal regime, the current framework is not sufficient. The issues of identification of perpetrators and attribution of malicious activities to specific actors in cyberspace merit specific considerations in the international legal context as does the challenge that damage is often caused when the perpetrator is not physically present. Dr. Li noted the importance of non-legally binding initiatives such as the International Code of Conduct on Information Security[4] and the Tallinn Manual[5] in the absence of international rules and regulations regarding these matters. He considers a code of conduct to be highly desirable. Additionally, he suggested that national law could play a role in addressing legal lacunae—for example, the promotion of robust national legislation (civil, criminal, commercial) on cyber issues could assist in laying the foundations for future international law developments.

The panel's discussion session explored various legal concepts, such as principles of damage and compensation. One participant enquired as to how, in the development of a national legal framework for cybersecurity, one determines who will pay compensation in the event of a cyberattack that results in damages? In response, another participant suggested that in order to even approach the subject of compensation, one would need to have a legally sound case for attribution, which is a challenge in the cyber domain. Another question raised was whether the ongoing development of the outer space legal regime may provide a beneficial reference for a cyber legal regime.

3 As described in Article 38 (1)(d) of the Statute of the International Court of Justice.

4 A draft of the International Code of Conduct for Information Security is available at http://nz.chineseembassy.org/eng/zgyw/t858978.htm.

5 For more information on the Tallinn Manual and Process, see https://ccdcoe.org/tallinn-manual.html.

Panel 3. Cyber Concepts

- **Cyber Sovereignty: Definitions and Application**
  Brig. (Ret.) Abhimanyu Ghosh, Director, National Security Council Secretariat, India
- **Cyber Boundaries: Reality or Fiction?**
  Mr. Ben Baseley-Walker, Programme Lead, Emerging Security Threats Programme, UNIDIR
- **Attribution: Linking Cyber into the Wider Security Picture**
  Dr. Tobias Feakin, Senior Analyst National Security and Director, International Cyber Policy Centre, Australian Strategic Policy Institute

Panel 3 examined some of the legal and political terminology frequently employed in international forums and processes relating to the cyber domain. Many terms are taken from more conventional legal contexts then modified and applied to cyberspace, such as cyber sovereignty, cyber boundaries, and attribution in cyber activities. Exploring the definitions and national-level understanding of these terms is essential for the progress of a cyber legal regime that is sound, comprehensive, and acceptable to all states.

Brig. Ghosh presented on the idiosyncratic nature of "cyber sovereignty" and the challenges therein. He began by exploring the challenge of reconciling the notion of sovereignty, which is territorial in nature, and the cyber domain, which is inherently borderless. Determining the extent of a given state's cyber sovereignty becomes even more difficult as a result of the diversity of actors in cyberspace (public, private, state, non-state, criminal, and terrorists among others), ambiguity over responsibility and deniability, issues with attribution, and ambiguity of jurisdiction in cyberspace—particularly as regards transborder data flows.

As a subset of cyber sovereignty, Brig. Ghosh sees data sovereignty as a key facet of international conversations on cybersecurity. This form of sovereignty relates to data generated or passed through national ICT infrastructure. Part of this discussion is the right to privacy in the digital age. Many consider data sovereignty as a human rights issue, with the privacy of individuals constantly being balanced with monitoring data in the interest of national security.

In conclusion, he noted the challenges in the cyber sovereignty conversation as defining the term itself, and in allowing the free flow of information while respecting the sovereignty of the state. He sees increased multilateral dialogue on this subject as vital to the development of a consensus-based definition and understanding.

Next, Mr. Baseley-Walker explored the concept of boundaries in the cyber domain and explained how they are inherently different from the boundaries in the physical domain. From the security perspective, developing a common international understanding on cyber boundaries is key to avoiding miscalculation and misattribution, which could result in conflict escalation with few mitigation controls.

Mr. Baseley-Walker identified three key aspects of cyber boundaries. The first aspect, the physical cyber domain, is perhaps the easiest to determine as ICT infrastructure has a physical base; in other words, it is possible for states to exercise sovereignty over the hardware within its borders. The second aspect is the origin point of cyber activities. This refers to the initial location of a cyber action which takes place in a physical space governed by a sovereign state. The third and last aspect is the impact point of cyber activities, which may take place outside the state from where the cyber action originated. An interesting

question is, if an individual carries out an activity within a state where that activity is legal but creates an impact in a state where that activity is illegal, what is the appropriate course of action? It may seem logical to apply the tenets of traditional criminal of law, but the nature of the cyber domain complicates this through its interconnectedness. For example, when a state carries out an activity that may have implications for the connectivity in another state, can one call this a cross-border impact? What would the legal implications be? What if a part of this activity was routed through a third state without their knowledge? What is this third state's responsibility to monitor such internet traffic? Questions like these are what complicates the notion of a cyber boundary and limits the development of concrete definitions.

In conclusion, Mr. Baseley-Walker argued that while the cyber domain may not fit inside the parameters of the Westphalian state system, on which international law, state boundaries, and international relations are built, it does not mean the international community needs to start afresh with the cyber boundaries conversation—further dialogue can help elucidate national perspectives and build consensus on the best path forward.

In the final presentation of the panel, Dr. Feakin explored attribution in cyberspace. He noted that while attribution is not entirely impossible in cyberspace, one may never be entirely certain when attributing a cyber action to one party—therefore, he saw many attribution cases as boiling down to a matter of judgment from governments acting upon evidence they have gathered, which in turn relies on the specific political climate in which the action took place. In his view, states can help manage this issue by prioritizing appropriate responses and ensuring that there is clear allocation of responsibilities within the government. In regions where the stakes are high for interstate relations, Dr. Feakin saw mitigating miscalculations emanating from the cyber domain as a chief concern.

He explained that the process of tracing a cyber activity and confirming attribution in cyberspace is multifaceted, involving at least four aspects:

- The **technical aspect** involves identifying the digital forensic trail to trace activity to an internet protocol (IP) address which can lead to locating the perpetrators; however, limiting traceability and hindering the identification process is often a fundamental part of malicious cyber activities.
- The **social/physical aspect** is the process of connecting an individual or group to the actual network or computer used to deliver the payload itself. However, if traced to a given person, they could claim their computer was stolen or their network was hacked.
- The **political aspect** involves implicating a particular state or actor in a cyber activity, which can be challenging in interstate relations. If a given state has traced a malicious cyber activity to another state, the original state must request assistance from the other state, which requires a cooperative linkage, a degree of goodwill, and time. During this period, evidence can be destroyed and the perpetrators may have time to escape.
- The final aspect is the **legal aspect,** which involves the creation of a legal case for responsibility and subsequent action. This is contingent on the strength of the three previous aspects and the specific legal system in which the case takes place.

Attribution in the cyber domain is a complex process that requires robust investigative measures and national-level legislation as well as cooperative interstate relations. Dr. Feakin

explained that, in the end, attribution of cyber activities is a matter of judgment that is contingent on the level of proof that a given government and public are willing to accept as reasonable for action.

The discussion period of the panel revolved around a deeper discussion of attribution in cyberspace. One participant noted that many states are capable of requesting, through legal orders, the cooperation of another state in a given case, however this relies on the health of the two states' political relations. In advance of more situations where states do not exchange information due to poor political relations, it is important to engage in dialogue and explore norms and common understandings for what responsible state behaviour should look like in the cyber domain. Another participant noted that at times the evidence is overwhelming for attributing a specific cyber activity to a given state, yet still a state may choose not to act due to tense political relations or fear of political consequences in other domains. This led to a discussion on the reality of bridging theory and practice in the cyber domain.

Panel 4. The Use of Force

- **Cyber Activities in the Context of Article 2(4)**
  H.E. Dr. Kriangsak Kittichaisaree, Ambassador, Ministry of Foreign Affairs of Thailand and Member of the International Law Commission of the United Nations, Thailand
- **Cyber Warfare: What Is It?**
  Mr. Richard Desgagné, Regional Legal Adviser for East Asia, International Committee of the Red Cross (Beijing)
- **Cyber Weapons: A Reality?**
  Dr. Cherian Samuel, Associate Fellow, Institute for Defence Studies and Analyses, India

Panel 4 explored a major topic in many national and multilateral discussions on state activity in cyberspace—the use of force. Panellists explored the legal underpinnings of the use of force and defining a cyberweapon under international law, as well as the ways in which cyber warfare can be understood in an IHL context.

Amb. Kittichaisaree discussed several key concepts relating to the use of force vis-à-vis the Charter of the United Nations, including how cyber issues fit into the concept of maintaining international peace and security of Article 1, the meaning of the term "use of force" under Article 2(4), and the meaning of "armed attack" under Article 51.

The international community is split between different schools of thought on how the law regarding the use of force should be applied to the cyber domain. On one hand, the Tallinn Manual is clear that cyberattack may at most lead to reprisals and countermeasures, as a cyberattack can never meet the threshold of armed attack. The ambassador considered that the United States position differs in that there is a right of self-defence in response to any use of force.

Amb. Kittichaisaree suggested that use of force inciting such a response must be of the gravest type, and the fact that an armed attack has occurred does not, alone, amount to an event that engenders the right of self-defence. In the context of cyberattack, he noted that the definition of aggression refers to the use of any weapon by a state against the territory of another state.

Amb. Kittichaisaree explained that currently there is no international consensus on whether a cyberattack is tantamount to an armed attack, which could be grounds to invoke Article 51. Additionally, there is no widespread consistent state practice in response to a malicious cyberattack. On matters below the threshold of an armed attack, countermeasures, retorsion, and reprisal may be permissible.

Mr. Desgagné presented on cyber warfare from the IHL perspective. As with many aspects of the cyber domain, he explained that there is currently no concrete definition for cyber warfare at the multilateral level. Nationally, many states have advanced definitions via national policy documents, however seldom in legislation. He noted the many references to "information wars", "information weapons", and "information operations"—however while many of these terms include common elements, they do not always coincide. In applying international law and invoking IHL, being able to distinguish between cyber warfare and cyber operations both during, and outside of, armed conflict has important implications; it is only in the context of armed conflict that the rules of IHL apply and impose specific restrictions on the parties to the conflict.

For the International Committee of the Red Cross (ICRC), cyber warfare is understood as the following: operations against a computer, or computer system, through a data stream when used as means and methods of warfare in the context of an armed conflict as defined under IHL. Mr. Desgagné noted that this definition excludes kinetic and physical operations directed against the material components of ICT infrastructure, and the use of cyberspace for communications, for example to transmit orders to other communication posts or the control of weapons using global positioning systems (GPS).

In times of armed conflict, the ICRC considers that IHL naturally applies, meaning any cyber operations taking place in the context of an existing conflict are governed by IHL. Consequently, cyberattacks taking place in these circumstances should only be directed at military targets, and precautions need to be taken to avoid civilian casualties. However, in the absence of an armed conflict, what events in the cyber domain could be considered equivalent to an international armed conflict and thus trigger IHL? As guidance, he offered several comments. In the event that a cyberattack causes damage outside of the origin state, similar to that of a kinetic attack, then determining whether it amounts to international armed conflict depends on whether the attack is attributable to a state and whether it amounts to "armed force"—a term not defined under IHL.

Some consider that if a cyberattack is attributable to a state and it causes the same level of damage as a kinetic attack, then it would be an international armed conflict. In the case of a non-international armed conflict in the cyber domain, he saw the main question as one of differentiating between criminal behaviour and armed conflict. In the absence of a treaty definition, he cited text from the International Criminal Tribunal for the Former Yugoslavia: a non-international armed conflict exists "wherever there is … protracted armed violence between governmental authorities and organized armed groups or between such groups within a state".[6] Furthermore, in order for an event to be considered a non-international armed conflict, it must fulfil two criteria: the armed confrontation must reach a specific, minimum level of intensity and the involved parties must show a minimum level of organization. In conclusion, Mr. Desgagné explained that the question of whether a pure cyber operation has the ability to trigger IHL is unclear, and will have to be elucidated in further discussions.

6 See www.icty.org/x/cases/tadic/acdec/en/51002.htm.

Next, Dr. Samuel provided an interpretation of the term "cyberweapon". Historically, conventional weapons were classified based on their ability to kill, injure, or disable, or cause destruction of property. Many weapons have been banned with the help of laws of armed conflict, but in the absence of such laws in the cyber domain, classifying and even determining a baseline definition for a cyberweapon is a challenge. A logical first step in cyberweapon regulation may be a cyber arms treaty to limit the development of offensive cyber capabilities; yet if this were to be enacted now, it may divide the world between the haves and have-nots of cyber capabilities.

Dr. Samuel explained that many criminal actors and national militaries are developing their offensive cyber capabilities, and called for more dialogue in the political realm about these military developments, as well as a concerted effort to determine technical, legal, and policy definitions for cyberweapons. He also called for more cross-pollination between interest groups and stakeholders involved in this conversation.

In the discussion period, one participant mentioned the Stuxnet virus, and enquired as to whether the virus crossed the threshold for an armed attack as it caused physical damage to an Iranian nuclear facility. A participant responded that it depended on which school of thought one followed, as illustrated by Amb. Kittichaisaree. Another participant posed the question, if a malicious cyber activity is carried out by an individual and not a state, do Articles 2(4) and 51 apply? The responses to this question were varied which illustrated the complexity when approaching even hypothetical questions, let alone real-world issues. One participant concluded the discussion by explaining that one can always find an example that undermines the principles of any legal regime, and therefore it is essential to have a strong and commonly understood foundation for action. Such a foundation, however, happens to be a fundamental challenge in the cyber domain.

Keynote Speech

- **Obligations, Rights, and Responsibilities in Cyberspace**
  Prof. Park Nohyung, Korea University

Prof. Park presented on the nature of state activity and engagement in cyberspace, including a state's obligations, rights, and responsibilities. He began by noting that there are currently no explicit treaties dealing with cyberspace, nor relevant individual areas of international law—with the exception of the Convention on Cybercrime. In the Asia-Pacific, he sees that members of the Shanghai Cooperation Organization are eager to conclude a similar regional international agreement on cyber conduct. In the multilateral context, the United Nations General Assembly has discussed aspects of cyberspace in the First, Second, and Third Committees as well as the ongoing GGE on ICT. Prof. Park viewed these regional and multilateral processes as beneficial to enhancing security and working towards a peaceful, stable, and prosperous cyber domain.

As regards the nature of state activity in cyberspace, Prof. Park referred to the work of the GGE on ICT. In its 2013 report, the GGE recommended that state sovereignty and the norms and principles that flow from sovereignty apply to state conduct in cyberspace. Among these norms and principles are the affirmation that states must meet their international obligations regarding internationally wrongful acts attributable to them. He agreed that existing international law, including the Charter of the United Nations, applies to cyberspace, and noted that that the recommendations from the report were endorsed by the General

Assembly, which points to a strong foundation for determining state obligations, rights, and responsibilities in cyberspace.

Prof. Park then shifted his attention to human rights in cyberspace. He mentioned resolutions that were adopted by the United Nations Human Rights Council in 2009, 2012, and 2013 that extended human rights to the cyber domain, discouraged the use of ICT for purposes contrary to respect for human rights, and called on states to align national legislation on cyber activity to comply with international human rights law. However, the real issue that Prof. Park sees is not so much whether current international rules apply to cyberspace, but how they apply and how they should be interpreted. He felt that common understandings on the application of international human rights law, and other forms of international law, should be further studied and that additional norms could be developed to reflect the unique characteristics of the cyber domain.

In conclusion, he recommended a further study of the application of existing international law in cyberspace and a higher level of participation from the private sector and civil society as part of a multi-stakeholder approach to Internet governance.

Panel 5. National Views on International Peace & Security Aspects of Cyber Issues

- **Australia**
  Ms. Julie Heckscher, Assistant Secretary, Sanctions, Treaties and Transnational Crime Legal Branch, Department of Foreign Affairs and Trade, Australia
- **Malaysia**
  Ms. Shariffah Rashidah Syed Othman, Principal Assistant Secretary, Cyber and Space Security Division, National Security Council, Prime Minister's Department, Malaysia
- **Japan**
  Mr. Ryohei Kanamaru, Deputy Director, Ministry of Foreign Affairs, Japan

The final panel explored various national perspectives on the international peace and security aspects of cyber issues. In driving the international law and cybersecurity conversation forward and building consensus on key issues, it is important to express national approaches and understandings on existing international law.

Ms. Heckscher began her presentation by acknowledging the difficult task ahead for policymakers and diplomats in developing robust international frameworks in pursuit of a stable and secure cyber domain. She acknowledged that ICTs are constantly evolving and outstripping the measures taken by governments and the international community.

To foster regional cooperation, CBMs, and deeper bilateral linkages, Australia is in favour of international collaboration and dialogue (including seminars such as this one). To widen participation in cybersecurity processes, incorporating voices from various stakeholders and not only states, Australia is in favour of a multi-stakeholder approach to Internet governance. Australia, which chaired the 2013 GGE on ICT, welcomed the recommendations from that year's report and felt that it was an affirmation that international law was a beneficial starting point for moving forward relevant cybersecurity and cyber law conversations. Furthermore, in terms of sovereignty and self-defence in the cyber domain, Australia feels that it is acceptable to exercise control over the physical ICT infrastructure within its territory, and that in the event of a cyberattack that meets Australia's interpretation of the threshold for

an armed attack, it could respond with whichever lawful means it deems appropriate using either cyber or kinetic means, or both. She stressed that in many situations, appropriate courses of action would need to be considered in light of specific circumstances.

Moving forward, she mentioned that Australia has been pleased to work with the Russian Federation, Malaysia, and various members of ASEAN and the ARF on the cybersecurity area of the ARF Counter-Terrorism and Transnational Crimes Work Plan. Australia would welcome more dialogue and work such as that plan, and the development of a framework for preventing, managing, and responding to cyber incidents. As a final comment, she noted that future initiatives on cybersecurity should be inclusive rather than exclusive.

Ms. Syed Othman's presentation focused on the technical and policy aspects of Malaysia's cyber governance. Due to its diversity of cultures, traditions, religions, and ethnic groups, Malaysia sees any abuse in cyberspace as a possible threat to national harmony and stability. As a result, the government has taken steps to ensure a safe and secure cyber domain, paying particular attention to the growth in organized cybercrime. The state has developed a national cybersecurity policy that determines which ICT infrastructures are important to the nation, and what the impacts of cyber-related destabilization may have on national defence and security, economic well-being, image and government function, as well as public health and safety. This policy informs the national threat level as regards cybersecurity.

Malaysia recognizes that no state is immune to cyberattack, and the potential for a spill-over effect, regionally or globally, is a reality. As such, Malaysia encourages continued cooperation among other states, and maintenance of trust and confidence in the cyber domain. In pursuit of this, Ms. Syed Othman provided an update on the progress of the ARF's Security of and Use of Information Technologies Work Plan. Malaysia has been working with Australia and the Russian Federation on this draft work plan, and in December 2014 planned to submit a copy to all ARF participating states. She hopes that this draft will soon be open to adoption by ARF states. She noted that Malaysia was happy with the progress of the work plan and believed that it would contribute to a peaceful, secure, and open ICT environment by developing trust among ARF states in the region. In conclusion, she reminded participants that Malaysia will hold the chairmanship of ASEAN in 2015 and that it plans to use this opportunity to play a role in strengthening cooperation in cybersecurity.

The final presenter, Mr. Kanamaru, provided the Japanese national perspective on cyber issues and the interaction with international peace and security. He explained that Japan sees the cyber issue as one that is difficult for any one state to address alone; it is essential that the international community address cyber issues together and establish rule of law in the cyber domain under the multi-stakeholder approach to Internet governance, with respect for universal values of freedom and democracy. Japan believes that international law, including the Charter of the United Nations and IHL, is applicable in cyberspace; however, further consideration is required for the specifics of how individual rules and principles can be applied. In the meantime, Japan believes it is important to begin building consensus on acceptable state behaviour in cyberspace, promoting CBMs, and preventing escalation caused by misunderstanding through the exchange of information regarding national cyber strategies and structures.

As a country with high Internet connectivity, Japan wishes to contribute more proactively in securing peace, stability, and prosperity in the cyber domain. Through international cooperation to ensure the free and safe use of cyberspace, Japan is engaging in the development of international rules, CBMs, and capacity-building, as well as participating in

the 2014–2015 GGE on ICT as well as the 2015 Global Conference on Cyberspace in the Netherlands. Additionally, Japan is working towards the establishment of CERTs in less developed states, particularly among ASEAN member states. As a party to the Convention on Cybercrime, Japan is working to widen subscription to this initiative.

The discussion panel explored some of the specifics of the Convention on Cybercrime, among other subjects. As Australia and Japan are both signatories of the Convention, one participant asked if there had been any noticeable difference in the way it helped a state to combat cybercrime. Another participant noted that in terms of transborder information gathering, the Convention had been incredibly helpful—and that collaboration between states was the most promising chance for limiting cybercrime. Another participant explained that if one state that is a signatory of the Convention requires information from a non-signatory state, information-gathering could be a challenge. Often, states have deep bilateral relationships or have exchanged memoranda of understanding on the subject to overcome such information-gathering challenges; however these are not necessarily the best mechanisms for quick and effective law enforcement responsiveness.

Scenarios

The final session of the Asia–Pacific Regional Seminar divided participants into groups and provided them with a hypothetical scenario involving transborder, malicious cyber activity.

One participant commented that this situation exemplified the importance of establishing points-of-contact in relevant government offices, aviation authorities, and civil society. There was resounding agreement that in these emergency situations, it was important to know nationally who is taking the lead and the type of technical expertise needed on a fact-finding team. One group focused on establishing cooperation among government agencies for an investigation. This group was interested in determining whether this event was attributable to a state or non-state actor. Another group focused on the specifics of compensation for the damages due to air traffic cancellations and general societal disruption. They discussed where one might direct the compensation request: directly to the accused state or to the International Court of Justice were two options. One participant argued that if the malicious cyber activity were attributable to a state, then it was within a state's obligations to the international community for this state to handle; insufficient response on the part of the state could be interpreted as encouragement of such activity.

The discussion period showcased various interpretations, understandings, and approaches that participants took in managing and responding to malicious cyber activity. The discussion also highlighted the value of involving multiple different branches of governance and professions when exploring options for the management of responding to such an event: an entirely policy-focused or legal-focused decision-making team could possibly lead to responses that do not comprehensively address the threat and therefore do not mitigate the full impacts.

Closing Remarks

The most common message heard throughout the seminar was the need for international cooperation in the cyber domain. The general sentiment found among seminar participants as regards international law and its application in cyberspace seemed to be that the international community is still unclear as to how to apply its tenets and principles. There is,

therefore, a very long way to go in this conversation, but seminars and regional conferences such as this are a positive step in building consensus. Mr. Baseley-Walker thanked the Republic of Korea for hosting this event and the participants for their active participation and willingness to tackle some very challenging issues.

International Law and State Behaviour in Cyberspace Series

Africa Regional Seminar

Conference Report

3–4 March 2015, Nairobi, Republic of Kenya

Introduction

As part of its International Law and State Behaviour in Cyberspace Series, UNIDIR carried out its Africa Regional Seminar on 3–4 March 2015 in Nairobi, Republic of Kenya.

Over the past two decades, there has been a growing reliance on cyberspace applications across a broad spectrum of activities and processes. As governments and societies increasingly depend on cyberspace in their daily activities, there is an urgent need to determine how existing international legal instruments and norms apply in the borderless and fast-evolving world of cyberspace. Among governments and in academia, there is a consensus that international law does apply in cyberspace; however the question remains: in what ways does it apply? In light of the 2012–2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) report—which noted the applicability of international law—and the convening of the fourth GGE in 2014–2015, it is an opportune time to explore this question and related conversations.

In pursuit of this, the Africa Regional seminar brought together both legal and policy voices to explore the cyber domain's legal context as it relates to the African region. This meeting provided an opportunity for regional stakeholders to exchange views and opinions, and to engage in a dialogue on the complexities and various interpretations of the applicability of international law in cyberspace within national frameworks. The seminar aimed to promote greater regional understanding, as well as to provide participants with a network of contacts throughout the region that in the long term might allow for better communication and cooperation on cyber issues.

PROCEEDINGS

Conference Chair

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

Welcoming Remarks

- **Ambassador Anthony Andanje**, Director, Multilateral Affairs, Ministry of Foreign Affairs, Republic of Kenya

Opening Remarks

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

Ambassador Andanje opened the seminar by extending to all participants a warm welcome from the Republic of Kenya and thanking UNIDIR for bringing the region together to discuss the important topic of cyber and international law. He noted that cyber is a growing resource on which all states are increasingly dependent, and there is a growing reliance on cyberspace applications throughout government and private sector activities. In addition to the significant contribution of the cyber domain to socioeconomic development, this rapidly developing area poses enormous challenges and risks. Ambassador Andanje outlined that today cyber warfare occupies a central position in the military doctrine of some states, as demonstrated by the substantial spending and resource usage being applied to creating advanced offensive cyber capabilities. In order to address the many challenges posed by the cyber domain, all states and stakeholders have a role to play in working towards cyber stability, part of which requires addressing critical cyber issues such as attribution and state responsibility. There have been key developments on state behaviour in cyberspace at multilateral and regional levels and that, with both the United Nations General Assembly resolution 5370 and the GGE, there is recognition that international law applies to state behaviour in the use of ICT.

Ambassador Andanje explained that Kenya is involved in both regional and international cooperation on key issues in the cyber domain, including being an active participant in the GGE, as Kenya considers that the group is contributing to significant changes at the multilateral level. He added that although Africa is facing several challenges on the policy and security aspects of cyber issues, it is critical that, as new and growing stakeholders, African states should participate effectively in developing parameters for responsible activity in the cyber domain in order to maximize national benefits in the long term. The adoption of the African Union (AU) Convention on Cybersecurity and Personal Data Protection in June 2014 was seen as a positive development and is a testament to the efforts being made in the region to craft legal instruments on cyber. Finally, he affirmed that all African states have a clear interest as well as a clear responsibility to uphold international law and maintain international order.

In Mr. Baseley-Walker's opening remarks, he underlined that cyber is the game changer of our age and something all states have an interest in. As an issue that cuts across multiple other subject areas, it is a challenging one to address and regulate. Unlike traditional areas of policy and law, the difficulty with cyber lies in the fact that, for many new entrants, approaches to policy and other initiatives have to be developed on three different levels

simultaneously: national, regional and multilateral. Indeed, today states may resort to using traditional policy processes ill-adapted to cyber, which is a fast evolving area, requiring decisions to be made in short time frames.

He explained that UNIDIR's International Law and State Behaviour in Cyberspace Series seeks to engage a broad spectrum of stakeholders, including those who perhaps historically have not had a major voice in international security and dialogue on cyber, and to provide a space for their input in pragmatic dialogue on the development and the applicability of international law to the cyber domain. By providing a platform for a regional discussion on issues that African states are facing in the cyber domain, it is hoped that participants could explore how cyber may be a destabilizing component in ongoing international security relations and consider how to mitigate the risk that cyber becomes a trigger for instability and conflict in the future.

Panel 1. Introductory Context

- **Why Cyber Matters in Africa—Looking to the Future**
  Ms. Dorothy K. Gordon, Director-General, Ghana–India Kofi Annan Centre of Excellence in Information and Communication Technology
- **Cyber and Development in the African Region**
  Dr. Towela Nyirenda-Jere, Programme Manager, e-Africa Programme, The New Partnership for Africa's Development Planning and Coordinating Agency
- **Obligations, Rights and Responsibilities in Cyberspace**
  Mr. Michael Katundu, Director of Information Technology, Communications Regulatory Authority, Communications Commission of Kenya, Republic of Kenya

A key aim for this seminar was to encourage an exploration of the issues most relevant to African states and to allow regional perspectives and differences to be discussed, thereby increasing understanding among neighbouring states. It sought to link the cyber conversation with the international policy climate, helping highlight the far-reaching impacts of cyber insecurity or instability in other realms of international relations. Panel 1 laid out the foundations for such discussions by expanding on the importance of cyberspace to both the African region's development and the international policy context.

Ms. Gordon presented on the importance of cyber in Africa and the steps that the continent must take for the future. She began by noting that cyber engagement is a question of survival for Africa and that states need to coordinate on this issue in order to develop ICT capabilities and adequate cyberspace regulation. She considers that cyber increasingly matters to Africa because African economies are becoming more integrated with the global economy, and cyber issues arising in one country can easily spread to others. As technological innovation spreads across the African region and more citizens gain access to the cyber domain, governments are exploring legal ways to best use and secure cyber technologies. However, dealing with the use of new technologies to provide services to citizens has put a tremendous stress on already stressed governments. The task of managing and protecting private data has become increasingly challenging—both for governments in terms of the rights and privacy of users, and for law enforcement agencies in conducting investigations. She noted that addressing the realms of the Internet where criminals reside is a global issue and governments must be aware of the risks and crimes posed by new technologies in order to create appropriate international and national legal instruments.

To address these new types of challenges that the continent is facing, Ms. Gordon laid out several recommendations: creation of a regional information-sharing mechanism on threats and risk mitigation; use of transparent security systems for critical national infrastructures; education of the public/private sector and governments on cyberspace; cooperation with the private sector; participation in global decision-making processes, and the development of national policies on cyber. Finally, she underlined the necessity of adapting, at a regional level, the multi-stakeholder models used at the international level.

Dr. Nyirenda-Jere then explored the relationship between cyber and development in the African region. The New Partnership for Africa's Development (NEPAD) has been conducting several projects to create capacity in the areas of cyber stability and security to enable states to address the issues and challenges brought by the use of this technology. She illustrated her presentation with an overview of NEPAD's strategic work in cyber within its e-Africa programme, which has a number of focus areas for ICT, including broadband infrastructures, capacity development, creating an enabling environment and e-applications and services.

One facet of NEPAD's efforts is improving terrestrial Internet connectivity between all capitals in the region, as at present most Internet data is routed via Europe. However, in connecting the capitals together, cross-border infrastructures and services present challenges in terms of regulation. To address this challenge, NEPAD, in coordination with the AU, has developed national Internet Exchange Points (IXPs), and the AU is encouraging the creation of subregional Internet exchange points to provide another level of aggregation. The IXPs will allow for local economies to have their traffic routed and managed locally by Internet service providers through their local infrastructures instead of routing traffic via locations outside the continent.

Dr. Nyirenda-Jere underlined that NEPAD also works to encourage a multi-stakeholder approach to Internet governance, and considers capacity-building to be a key element in dealing with cyber issues globally. In 2013, NEPAD created the African School on Internet Governance to address the education gap; however, it was noted that capacity-building in national higher education systems in Africa is still missing. In summation, Dr. Nyirenda-Jere encouraged states to work with a multi-stakeholder or multisectoral approach, and to trust the various stakeholder groupings in the area.

Mr. Katundu's presentation addressed the issues related to obligations, rights and responsibilities in cyberspace. He started his presentation by referring to the World Summit on the Information Society (WSIS) of 2003 and 2005 organized by the International Telecommunication Union (ITU), where states recognized that "all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet". He explained that Kenya has developed a number of policies, strategies, institutions and frameworks towards these goals. He indicated that within the current "Vision 2030" strategy for development that Kenya is implementing, ICT does not constitute one of the three pillars; however, it is part of every pillar—and the Vision's objectives cannot be achieved without ICT. He indicated that Kenya has also created an ICT regulatory authority and a national Computer Incident Response Team (CIRT), both of which are playing key roles in the development and implementation of policies, laws and regulations for cyber security.

Mr. Katundu outlined that in developing relevant policies and legal instruments for the promotion and use of a safe cyberspace, governments must consider the obligations, rights and the responsibilities of citizens. When using ICT, citizens must remain protected, and

therefore governments must develop national policies and educate citizens on these rights and responsibilities. Governments must also implement laws and regulations in accordance with international law on new areas such as e-transactions, consumer protection, data and privacy protection, and cybercrime—in order to address the challenges these new areas pose to citizens.

In addition to the legal and policy framework, Mr. Katundu stressed that governments must ensure that various technical and policy aspects are addressed, including identification and protection of national critical information infrastructure; progress towards local, regional and international cooperation and collaboration on cybersecurity incidents; the development of international standards and legal principles on cybersecurity and related technologies; a coordinated technology watch and early warning network; capacity-building across all areas dealing with ICT; and the creation of consumer awareness in the use of new technologies. Finally, Mr. Katundu noted that achieving a safe and secure cyberspace is a collaborative effort and all cyber stakeholders have a role to play.

The discussion period raised questions on the challenges associated with coordination between intelligence and security agencies, and the necessity of capacity-building. In the area of intelligence and security, one participant suggested that all public and private cyber stakeholders should be brought together to coordinate with each other. Another participant noted that there is no best practice yet when it comes to guarding against infringement of citizens' rights with respect to their data, and that without regulation, this situation can lead to abuse. On capacity-building, one participant emphasized that this must be implemented in every sector of a society, with specific needs identified in order that any training or strategy developed can address needs in a targeted way. Another participant noted that education in ICT and cybersecurity was a key component for capacity-building in cyberspace and that states should start educating and training their citizens to develop capabilities and expertise.

Panel 2. The Legal Landscape

- **International Law and Cyber 101: An Introduction**
  Ms. Angela Ng'ang'a, Corporate Affairs Lead ESA and IOI, Legal and Corporate Affairs, Middle East and Africa, Microsoft Corporation
- **Current Mechanisms for Addressing Cyber at the Africa Regional Level**
  Ms. Amazouz Souhila, Senior Radio Transmission and Broadcasting Office, Infrastructure and Energy Department, African Union Commission
- **Regime Coherence: National, Regional and Multilateral Legal Interaction on Cyber Issues**
  Mr. Preetam Maloor, Strategy and Policy Advisor, International Telecommunication Union

Panel 2 tackled some of the major topics and questions raised by legal experts and states in the application of international law to the fast-moving and borderless cyber environment. From the private sector to governments, the issue of cyber requires the re-examination of the definitions of national and international principles, and the implementation of legal frameworks and mechanisms at the national, regional and international levels to regulate the challenges encountered in cyberspace.

Ms. Ng'ang'a opened the panel with a presentation on the basics of international law and cyber, and given her particular expertise, provided participants with information on how Microsoft regards legal obligations and consumers rights. Microsoft has been tackling the specific issues of cybercrime and cybersecurity a great deal, including establishing a digital crimes unit to explore how they can support customers and governments with understanding how to deal with the various new trends in technology.

Ms. Ng'ang'a noted that as the pace of activity in cyber increases, so does the likelihood of governments misinterpreting the actions of one another, and the risk of a cyber war cannot be discounted. She outlined that as cyber threats continue to grow, governments are looking at the ways in which they can protect their citizens. This tends to increase the need for access to data for law enforcement and intelligence matters, however governments may also exploit networks for a number of other reasons including economic espionage, military espionage and operations. Considering this, Microsoft has found that an increasing number of states are developing both defensive and offensive cybersecurity capabilities to prevent and fight back against cyber attacks.

Against this backdrop, Microsoft promotes the establishment of international cybersecurity norms to limit the potential of conflict in cyberspace and to define what state behaviour in cyberspace should be with regard to international law, so that events do not escalate to warfare. Ms. Ng'ang'a shared with the panel several norms that Microsoft promotes: states should not target ICT companies to insert vulnerabilities, or take actions that would undermine public trust in products and services; states should have a clear policy for handling privacy issues and security vulnerabilities with a mandate to report to vendors rather than to stockpile or exploit them; states should exercise restraint in developing cyberweapons and should ensure that any that are developed are limited, precise, and not reusable consistent with the concept of "distinction, discrimination and distribution" to limit the impact associated with these actions; states should commit to non-proliferation activities related to cyberweapons; and finally, that states should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Next, Ms. Amazouz explored the current mechanisms for addressing cyber at the African regional level. She noted that while African countries' access to broadband and Internet has increased, issues related to cybersecurity and cybercrime are still emerging. In many countries there is a lack of know-how in terms of cybersecurity and an inability to monitor and protect local networks, making African countries particularly vulnerable to incidents of cyberterrorism and cyberespionage. She suggested that for some states there is an inability to develop the legal frameworks to fight cybercrime, and for others, the level of implementation of legislation and deployment of security systems in the private and public sectors is low.

The presentation then showcased the work of the AU, which encourages states to cooperate and to combat cybercrime through a multi-stakeholder approach, involving both governments and industries. She added that considering the international dimension of cyber security, it is important to reinforce international cooperation on this issue particularly with regard to confidence-building measures (CBMs). To this effect, the AU has adopted a convention to address the cyber issue and to mitigate the risks deriving from misuse of ICTs. The objective is to define a regional harmonized framework for cybersecurity legislation, to develop general principles as specific provisions related to cyber legislation, to outline cyber legislation measures required at the member state level, and to develop general or specific provisions on international cooperation related to cyber legislation. The convention

embodies all aspects of cyberspace, including organization of e-commerce, the protection of personal data, the promotion of cybersecurity, and the fight against cybercrime. In this latter regard, the criminal provisions of the convention specifically set out definitions of ICT offences and adapt certain sanctions for ICT offences.

Ms. Amazouz stressed that the AU is also focused on assisting states in setting up their national legislation. By adopting the AU convention and transposing it into national policies, the different model laws and guidelines implemented by states will allow for the development of a more harmonized regional legal framework built on minimum common standards, principles and procedures in the regulation of cyberspace and the fight against cybercrime.

Mr. Maloor's presentation then focused on national, regional and multilateral interactions on cyber issues. Mr. Maloor outlined that facilitating the formulation of national strategies is key to creating effective measures for cybersecurity and stability. In this regard, the ITU works with ICT ministries to help set up ground infrastructures and basic capacity levels. Believing that capacity-building is a central foundation for cyber stability and security, the ITU provides states with technical assistance on mitigating risks, identifying best practices in legislation, and information-sharing. One initiative the ITU has launched is a subregional programme called "Support for Harmonization of the ICT Policies in Sub-Saharan Africa" (HIPSSA) to provide states with adapted responses for cyber incidents and to establish harmonized policy along with legal and regulatory frameworks at the regional and continental levels. The goal of this programme is to create an enabling environment that will attract investment, to foster the sustainable development of competitive African ICT regional markets and infrastructures, and to increase access of its people to related services.

In addition to these flagship projects, the ITU also provides in-country technical assistance for transposing international and regional guidelines to accommodate national specificities; has produced a guide to understanding cybercrime; carries out capacity-building under the coordination of the World Bank; and provides national assessment as well as public–private cooperation through national CIRTs. With regard to cooperation, Mr. Maloor emphasized that to have a global, effective level of cybersecurity, a coordinated, multilevel approach is needed. While Africa is doing well at the international and regional levels, it requires assistance in the implementation of relevant measures at the national level.

The discussions from this panel centred on the legal issues of privacy and vulnerability in the use of ICTs, and on the work of the AU to ensure the development of global legal norms and provisions. One participant enquired about the legal obligations of companies to provide secure technologies to governments and citizens. Another responded that privacy is critical, and that companies such as Microsoft work to ensure the integrity and reliability of their data and systems as they are entrusted by customers to hold their data. On the role of the AU to create global legal norms, one participant asserted that the AU believes cybersecurity is a global matter and thus should be managed in a global and integrated way. Accordingly, it was noted that the AU convention calls for all African states to be part of the process by setting up their national strategies in a way that involves all stakeholders and civil society.

Keynote Speech

- **African Imperatives in Cyber Norm Development**
  Dr. Katherine Getao, Information and Communications Technology Secretary, Ministry of Information and Communications Technology, Republic of Kenya

Dr. Getao's keynote presentation centred on African imperatives in cyber norm development, and outlined the importance of establishing cyber norms. She noted that as states are increasingly asked to take responsibility for certain aspects of cyberspace, it is necessary to define their sphere of responsibility. Even though the GGE affirmed that national laws apply to cyberspace, the interpretation and the application of laws remains an ongoing issue. She stressed that cyberspace and security are important items on national agendas, and cooperation among states will enhance regional and international agendas.

Looking briefly at the East African regional cyber landscape, she explained that there are some regional bodies and processes already in place, and that states recognize the importance of CIRTs as well as the importance of national strategy and implementation plans on cyber issues. She remarked that in this subregion national processes on cyberspace and cybersecurity are much more supported, advanced and robust than regional and international processes, as the multi-stakeholder approach requires time for institutions to learn to work together. Furthermore, there were seen to be multiple regional organizations working on cyber issues in East Africa, and each and every state is part of one or more of them, which adds complexity to harmonization and implementation. She suggested that, more broadly, cyber norms could be developed through the framework proposed by the AU convention, which calls for a definition of the role of governments, the development of policies and plans, provision of a broad legal framework for drafting national legislations, the identification of relevant authorities and institutions, and the outlining of important principles for cyberspace.

As a way to move forward, Dr. Getao laid out several recommendations: the creation of awareness- and capacity-building programmes; the implementation of a cyber norm agenda from the AU convention within national governments; and the possible creation of an AU Group of Governmental Experts in regional security and diplomacy in cyberspace. This latter proposal was largely supported by participants during the floor discussion.

Panel 3. Cyber Concepts

- **Attribution in Cyber: Responsibility for State and Non-State Activities**
  Ms. Jemima Njeri, Senior Researcher, International Crime in Africa Programme, Transnational Threats and International Crime Division, Institute for Security Studies Africa
- **Improving Cyber Access: Possible Threats and Challenges**
  Mr. Kodzo Gadzekpo (Marcus) Adomey, Education and Research Manager, AfricaCERT
- **Chain Reactions: Understanding Knock-on Effects in Cyberspace**
  Mr. Jonathan Ledgard, Director, Afrotech, École Polytechnique Fédérale de Lausanne

Panel 3 examined the basis for some of the legal and political concepts frequently employed in international forums and processes relating to the cyber domain. Some of the most discussed key concepts are attribution and responsibility in the cyberspace environment.

Exploring the issues encountered with these concepts when viewed in the context of cyber activity is an essential step to addressing the main challenges and ultimately to applying these terms to the cyber environment.

Ms. Njeri focused her presentation on attribution in cyberspace, specifically looking at responsibilities for state and non-state activities. She began by saying that in the context of international law, attribution is an essential and indispensable action, yet attributing certain cyber attacks to a specific actor can be difficult, or in the case of well-funded militaries, impossible, as the identity of perpetrators can be easily disguised and the origination point of the attack hidden. She noted that following a cyber attack accusations may be addressed without sufficient technical evidence or basis, which, in the case of state actors, may lead to a loss of mutual trust detrimental to international relations.

Ms. Njeri explained that the complex challenges associated with cyber attacks include problems perceiving an attack's seriousness and motive, justifying appropriate responses, and identifying the appropriate legal frameworks that may apply. She considered that there are several factors that complicate the task of attribution in cyberspace. Firstly, cyberspace is a domain for both state and non-state actors, and they may carry out activities of diverse sophistication for a variety of purposes. Secondly, many cyber tools can be used for either legitimate or illegitimate purposes. Thirdly, the private sector is an increasingly major player in the domain, both involved in Internet controls as well as providing the systems and private platforms upon which states rely. Fourthly, there is no common understanding on applicable international rules and standards for state behaviour in the cyber domain.

Ms. Njeri underlined that depending on whether an attacker is a state, non-state or proxy actor, various aspects of international law may be applicable. In this regard, it is necessary to evaluate the role of international regulation, and to identify the technical and regulatory problems of attribution, as well as to explore possible solutions to cyber attacks when attribution cannot be achieved. She saw the absence of an international legal regime for cyberspace as a great challenge in terms of dealing with issues of attribution, and expressed that there is a necessity for not only an international legal framework, but also regional and national ones.

Mr. Adomey's presentation explored the possible threats and challenges to improving cyber access. He defined such threats and challenges as cyber "determinants" and identified three types of determinants:

- **Technological determinants** that are relevant to an organization to improve cyber access.
- **Organizational determinants** that are the characteristics and resources of an organization.
- **Environmental determinants** defined by the structure, the regulation and the level of technology service providers of an organization.

Although he sees a high level of politicization of cybersecurity issues, Mr. Adomey noted that it remains a low priority area in most states, as evidenced by the porosity of laws and the slow speed of processes establishing them. In order to address these challenges, he recommended that states enact measures to increase national awareness, to promote the development of technical skills in the region, to build strong and depoliticized cybersecurity institutions, to participate in a regional security strategy, and to create effective computer

emergency response teams (CERTs). Finally, he proposed that states should consult, collaborate and cooperate with each other, with trust, to ensure overall cybersecurity.

Mr. Ledgard closed out the panel by sharing his perspectives on the possible future of African countries with regard to the development of Internet technology and high connectivity. He suggested that in the future a generation of Africans with low incomes but a high degree of Internet connectivity could generate large political dissonance across the continent. He felt that a lot of work in the region is still needed to ensure the security and safety of the cyber domain, especially considering that in future it will not only be a major space for communication but for commerce as well. As an example, Mr. Ledgard explained that the development of new technology such as cargo drones could allow the movement of goods more efficiently, effectively, and economically across the continent, which would be a revolutionary option for African economies. However, he noted that using cargo drones requires a high degree of connectivity that could expose the system to vulnerabilities.

The discussion session of this panel focused largely on the issue of attribution. One participant asked if there was any possibility of finding a methodology such as the one used in the traditional legal domain to enable prosecution even if complete certainty of guilt or innocence cannot be secured, and to consider the implications of punishing those that failed to protect when obligated. Another participant responded that, unfortunately, attribution is so broad that it can entail issues with political implications, therefore certainty appears to be mandatory, and thus called for policies, standards and guidelines to obtain and ensure this certainty. It was also raised that the problem of attribution is a technical one in terms of the available tools to trace the origins of a cybercrime that involve some illegal use of technology.

Panel 4. Cyber Stability

- **Cyber Conflict and International Law**
  Dr. Nils Melzer, Senior Advisor, Security Policy Division, Political Directorate, Swiss Federal Department of Foreign Affairs, Swiss Confederation
- **An Arab African Perspective on Multilateral Approaches to Cyber Conflict and Cybersecurity**
  Mr. Amr Aljowaily, Minister Plenipotentiary, Permanent Mission of Egypt to the United Nations in New York, Arab Republic of Egypt
- **The Role of Cyber in International Peace and Security**
  Dr. Eneken Tikk-Ringas, Senior Fellow for Cybersecurity, International Institute for Strategic Studies: Middle East Office

Panel 4 explored a major issue in many national and multilateral discussions on security in cyberspace—stability. Panellists explored the legal underpinnings of the use of force in cyberspace and defining cybersecurity under international law, as well as the ways in which cyber warfare can be understood in both the United Nations and international humanitarian law context.

Mr. Meltzer's presentation explored international law instruments applicable to cyber conflict. He identified several bodies of law that are applicable in the area of cyberspace, among which are the Charter of the United Nations which prohibits the use of force in international relations, international humanitarian law in armed conflict, and the obligations and rights of neutral states in conflict. Mr. Meltzer underlined the significance of the definition of the

use force in cyberspace for states, as they can only resort to self-defence if force is used against them in the sense of the Charter. However, if this threshold is not met, states can still use countermeasures that are below the generally-agreed United Nations threshold of the use of force. He added that if use of force is actually perceived in cyberspace by a state, the law of conflict would be applicable.

With regard to international humanitarian law, Mr. Meltzer asserted that a distinction must be made between civilian and military persons and objects, and explained that an attack is defined as an "act of violence in offence or defence". In this context, it could therefore be argued that states cannot legally attack civilian data and infrastructures in cyberspace. He noted that while there are difficulties in literally applying the existing treaties, there is common agreement that international humanitarian law can apply to cyberspace, however the difficulties lie in identifying the underlying legal principles.

Mr. Aljowaily presented an overview of multilateral approaches to ICTs and international peace and security. He started by emphasizing that it is important to understand that states conceptualize their international security policy according to different security paradigms and perspectives. Some states, for example, use three points of departure when addressing a cybersecurity issue: national security, homeland security and human security; and when analysing their national interests, states rely on the perception or evaluation of the magnitude of threats in the determination of policy.

Within the United Nations framework, he added, there exist three different perspectives for dealing with international security issues and international peace and security issues in general:

- regulation/arms control versus disarmament perspectives;
- trust and confidence-building measures versus prevention of an arms race; and
- pacific settlement of disputes

Mr. Aljowaily underlined that the threshold of definition for the use of force in cyberspace is not very high, considering that developing countries that have a lack of resources to address cybersecurity challenges posed by new technologies are far more vulnerable than developed countries to any form of disruption that may happen. He explained that in the context of ICT security the threat or use of force would also encompass the destruction or harm, in any form, of any of the three interlinked layers of the Internet, namely telecommunications and related infrastructure; technical standards; and content and its related applications. He considered that any form of deliberate disruption of one of these three layers can amount to a use of force, and thus fall under article 2 (4) of the Charter of the United Nations.

Finally, Mr. Aljowaily endorsed regular institutional dialogue on ICT security issues with broad participation under the auspices of the United Nations, as recommended by the GGE; and with regards to attribution, he underlined that all states must participate in all arrangements related to the management and governance of critical Internet infrastructure and Internet governance mechanisms.

Ms. Tikk-Ringas then discussed the role of cyber in international peace and security. She saw cybersecurity as broad and composed of technical as well as non-technical aspects which, in her opinion, explain why international cybersecurity consists of a number of questions that simultaneously involve many areas. She asserted that from a national perspective there are different priorities, capabilities and issues which every government should identify so that

the international community can understand how they can be comprehensively addressed to fit into regional conversations, consensus, and potentially, common international understanding and principles. She also encouraged the international community to embrace inclusive dialogue that would encompass governments alongside individuals, associations, enterprises and other organizations active in the private sector.

Ms. Tikk-Ringas remarked that we have entered a period in which it has become normal for states to develop military cyber capabilities, and that today cyber might be used in armed conflict or to pursue political goals. In such a context, she believes the international community can rely on several types of binding and non-binding international legal instruments to regulate and secure cyberspace. While there are 250 existing instruments adopted by different international organizations on the issue of cybersecurity, Ms. Tikk-Ringas encouraged states to think about how to resolve issues nationally or regionally, and to adapt international norms to specific contexts. She cautioned that everything could not always be decided at the international level, but that any chosen decisions should always be guided by law.

The discussion session explored the principle of territorial sovereignty in cyberspace, the perception of threats and the relevance of the Geneva Conventions to cyber activities. One participant asked if national territorial integrity applies to cyberspace and how one might define cyber attacks or incidents in terms of a threat to a state's security. One participant responded that in terms of sovereignty states are bound to existing principles, therefore the real question lies in how states interpret the concept of sovereignty. Another participant noted that within the three layers of the Internet, sovereignty applies predominantly to telecommunication infrastructures. With regard to the magnitude of threats, the participant considered that the lower the threshold is, the more developing countries are protected. Finally, one participant explained that the original Geneva Conventions were drafted to regulate relations and conflicts between states, however nowadays, actors in armed conflicts are no longer only states. Thus, it was suggested that international humanitarian law must evolve in its normative content and in its application of norms and principles to new technology.

Panel 5. Cyber and International Peace and Security: National Approaches to Legal Development

- **Republic of Cameroon**
  Ms. Balbine Manga, Attorney and Information and Communication Technology Consultant, Organisation Internationale de la Francophonie
- **Republic of Rwanda**
  Ms. Florida Kabasinga, Senior Legal Advisor, International Crimes Department, National Public Prosecution Authority, Republic of Rwanda

The final panel explored various national developments and perspectives on the international peace and security aspects of cyber issues. In driving the international law and cybersecurity conversation forward and building consensus on key issues, it is important to express national approaches and understandings on existing international law.

Commencing this panel, Ms. Manga presented the Cameroonian national perspective on law in cyberspace. She remarked that the geographical localization of the country in central Africa makes it an interesting example, as it shares boundaries with more than five countries.

She explained that cyber is one of the problems shared across borders in the subregion, while mobile connectivity and the high use of social media also bring new threats to the country.

She mentioned that Cameroon has implemented national institutions in charge of cybersecurity and the national legal framework is inspired by the Economic Commission for Africa (ECAS) regional framework. The laws encompass issues related to the use of ICTs, to cybersecurity and criminality. However, Ms. Manga recognized that all these actions have yet to be implemented, and Cameroon, as in the case of many other countries, does not have sufficient capabilities to do so. Ms. Manga summed up that all institutions, at the national and regional levels, should work together in sharing practices, implementing laws and building capacities.

Speaking on the perspective of Rwanda, Ms. Kabasinga stated that cyberspace is regarded as an essential component for Rwandan economic development and its future. ICT penetration is very high in Rwanda and almost everything is available online. Ms. Manga noted that throughout all sectors there is a gap in awareness of what cybercrimes are and the endless possibilities of them, and yet at the same time the latest developments in technology are still embraced.

To tackle the challenges posed by cyberspace, Rwanda has created a legal framework that includes laws related to cybercrime. At the organizational level, the state has created specialized institutions and is trying to undertake capacity-building in all institutions dealing with cybercrime prosecution.

The final panel discussion revolved around the difficulties encountered in investigation and prosecution of transborder cybercrime. When not dealt with at the political level, the processes of investigation and prosecution rarely proceed, due to the lack of international mutual legal assistance for extradition on one hand, and the costs and benefits of dealing with the cases compared to the damages they create on the other hand. Unless a particular case involves high-impact crimes, most cases are rarely fully prosecuted, and often the victims are the first ones to give up on pursuing legal resolution.

Scenarios

The final session divided participants into groups and provided them with a hypothetical scenario involving transborder, malicious cyber activity. There was resounding agreement that in these emergency situations it was important to conduct forensic inquiries to identify the critical infrastructures that attacks were coming from through national CIRTs or regional organizations. Diplomacy and mediation were favoured as appropriate national approaches to the issue, and requests for extraditions were encouraged to prosecute the responsible individuals. One group focused on establishing cooperation with neighbouring states and regional organizations to identify the nature of the incident, and to ascertain if other states might have been victims as well. It was noted that if the problem appeared to be between states, it would be a political problem that needed to be dealt with diplomatically; if not, existing national institutions might be best suited to handle the matter. Another group discussed the crisis management response at the national level and the necessity for governments to publicly demonstrate their efficiency in containing the situation. The group proposed the possibility of establishing national tribunals dealing with specific cybercrime issues.

The discussion period showcased various interpretations, understandings, and approaches that participants took in managing and responding to malicious cyber activity. The discussion also highlighted the need for cooperation to extradite cybercriminals when they are not state-aligned. Overall, participants emphasized the use of diplomacy and other countermeasures that do not include force as the favoured primary national approaches.

Closing Remarks

The most common message heard throughout the seminar was the need for international cooperation and mutual legal assistance in the cyber domain. The general sentiment found among participants as regards international law and its application in cyberspace seemed to be that the international community needs to create norms and guidelines which governments can rely on in order to apply the concept and principles of international law within their national context. There is, therefore, a very long way to go in this conversation, but seminars and regional conferences such as this are a positive step in building consensus and enhancing cooperation in new difficult areas.

International Law and State Behaviour in Cyberspace Series

Eurasia Regional Seminar

Conference Report

3-4 June 2015, Muscat, the Sultanate of Oman

Introduction

As part of its International Law and State Behaviour Series, UNIDIR carried out its Eurasia Regional Seminar on 3–4 June 2015 in Muscat, the Sultanate of Oman.

Over the past two decades, there has been a growing reliance on cyberspace applications across a broad spectrum of activities and processes. As governments and societies increasingly depend on cyberspace in their daily activities, there is an urgent need to determine how existing international legal instruments and norms apply in the borderless and fast-evolving world of cyberspace. Amongst governments and academia, there is a consensus that international law does apply in cyberspace; however the question remains: in what ways does it apply? In light of the 2012–2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE on ICT) report—which noted the applicability of international law—and the convening of the fourth GGE on ICT in 2014 and 2015, it is an opportune time to explore this question and related conversations.

In support of this goal, the Eurasia Regional seminar brought together both legal and policy voices to explore the cyber domain's legal context as it relates to the Eurasia region. This meeting provided an opportunity for regional stakeholders to exchange views and opinions, and to engage in a dialogue on the complexities and various interpretations of the applicability of international law in cyberspace within national frameworks. The seminar aimed to promote greater regional understanding, as well as to provide participants with a network of contacts throughout the region that, in the long term, might allow for better communication and cooperation on cyber issues.

PROCEEDINGS

Conference Chair

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

Panel 1. Introductions

- **Welcoming Remarks**
  Mr Eng Badar Ali Al-Salehi, Director General, Oman National CERT, Head of ITU Regional Cyber Security Center, Oman

- **Opening Remarks**
  Mr Jarmo Sareva, Director, United Nations Institute for Disarmament Research, UNIDIR

- **The Role of Cyber in International Peace and Security**
  Mr Ben Baseley-Walker, Programme Lead, Emerging Security Threats Programme, UNIDIR

Mr Al-Salehi opened the seminar by extending to all participants a warm welcome from the Sultanate of Oman and the International Telecommunication Union's Arab Regional Cybersecurity Center (ITU-ARCC), thanking UNIDIR for organising this regional seminar to facilitate the dialogue on important issues of cyber and international law. He expounded how the Sultanate of Oman started to address issues of cyberspace and cybersecurity on the basis of five main strategic pillars, including the establishment of organizational structure, capacity building, implementation of technical cybersecurity measures, fostering regional and international cooperation and, most importantly, the development and creation of national legislation. In this context, Oman's recently enacted cybercrime legislation of 2011 was mentioned.

Mr Sareva, Director of UNIDIR, welcomed all participants and expressed the institute's appreciation to the government of the Sultanate of Oman as well as the ITU-ARCC for their support in organizing the seminar. He emphasized the growing importance of the Arab Regional Cybersecurity Center as key component of the ITU's regional policy infrastructure. Next, Mr Sareva emphasized the progress and the changes the internet has brought to the daily lives of citizens around the globe, referring to the developments as 'Information Revolution'. Digital interconnectivity, connecting private actors, governments and international institutions alike, was described as a key characteristic of today's global economy, and thus, indispensable for economic stability and global development. He noted, however, that the growing dependence on Information and Communications Technology (ICTs) also bears risks. Mr Sareva noted that there is a steady annual increase in cybercrime, malicious use of cyberspace, and cyber attacks worldwide, leading to increasing instability and economic losses, and thefts of national security information. As governments and national defence agents are becoming increasingly dependent on networked ICTs, vulnerabilities arising thereof have become not only matters of national security, but potentially of international stability at large. The cyber domain is consequentially increasingly considered an extension of the traditional international security environment. Today, cyber resources form an integral part of many states' defensive arsenals and, in many cases, are now being factored in to military and strategic calculations, which may include both preventive or offensive capacities. This reality needs to be addressed by the international community at the multilateral level, according to Mr Sareva. In this context he noted that numerous efforts to forestall potential threats emanating from so called 'cyberweapons' that have been made by national, regional

and international actors, for example by initiatives such as the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Mr Sareva stressed that the consensus on the applicability of international law needs to be broadened to one about the implications as to *what* that means. Mr Sareva emphasised the timeliness of the seminar reiterating that a stable cyber domain is as a global endeavour. UNIDIR's long history of working on new threats and challenges and its standing as an impartial and independent voice within the United Nations were highlighted as essential to support States and other actors in developing practical, innovative thinking needed to facilitate the finding of solutions to existing and future challenges. Mr Sareva highlighted that UNIDIR aims to broaden its engagement with the Eurasian and Middle Eastern regions on matters of cyber stability and other issues of peace and security. In this context he expressed his appreciation to convene such intra-regional dialogue on policy and legal aspects of cyber stability and his hope for prosperous and interactive discussions during the seminar.

Mr Baseley-Walker continued by stressing the importance of the cyber domain for international peace and security and he emphasised the importance of initiatives that foster dialogue. The purpose of these regional seminars was described as to provide a platform for the facilitation of an open discussion to explore the positions, concerns and thoughts of individuals and countries on the role of cyber stability. He noted that cybersecurity is a collective concern that cannot be ensured at the national level alone. In light of the growing importance of cyberspace he noted that it is crucial to clarify how legal and policy measures can work together, both at the regional and the global level. Mr Baseley-Walker noted further that maintaining long-term access to the economic, social and other benefits of the cyber domain is a key imperative. He regretted, however, that a vast majority of voices of the international community have not been heard on this issue. Providing a forum for exchange between countries in specific regions is one way in which UNIDIR aims to open up the dialogue to actors that have been less vocal thus far. These discussions are intended to feed back into the multilateral environment and aim to ensure that the conversation on cyber governance does not continue to be dominated by a small number of principal actors. Another issue raised was countries' response mechanisms to both deliberate state-sponsored cyber attacks, and other forms of malicious cyber-activities. It was highlighted that UNIDIR perceives international security in the cyber domain as a balancing act between two important questions: how to benefit from cyber capabilities whilst preventing political tension between governments or non-state actors from spreading into the cyber-domain, risking to destabilize the international system and ultimately exacerbating the risk of physical conflict. Mr Baseley-Walker underlined hereby the necessity to create more clarity on this particular topic and acknowledged, again, the important role of regional initiatives, such as the ITU-ARCC and the Information Technology Authority (ITA). He closed the panel by stressing the Sultanate of Oman's trailblazer role as a growing hub on this issue in the region.

Panel 2. The Legal Landscape

- **International Law and Cyber 101**
  Dr Nils Melzer, Senior Adviser, Division for Security Policy, Directorate of Political Affairs, Federal Department of Foreign Affairs, Switzerland
- **Applying International Law to Cyberspace: Lessons from History and Doctrine**
  Dr Andrii Paziuk, Assistant Professor and Chair of International Law, Laboratory of Internet Governance (LIGO) Ukrainian Association of International Law
- **Proposed Legal and Policy Initiatives for Peace and Security in the Cyber Domain**
  Dr Marten Zwanenburg, Legal Counsel, Ministry of Foreign Affairs, Netherlands

Panel 2 addressed some of the major issues and concepts raised by legal experts and states regarding the application of international law to the fast-evolving and borderless cyber environment. The specifics of the cyber realm require the re-examination of national and international legal principles and the panel provided an overview of ongoing initiatives.

Dr Nils Melzer focused in his presentation on general principles of international law and the questions arising from their application to the sphere of cyberspace. He highlighted the existing consensus of legal experts and states on the applicability of international law to cyberspace and referred to the report by the GGE in the Field of Information and Telecommunications in the Context of International Security of 2013. He stressed, however, the importance of clarifying the implications of such a consensus on the applicability of the law and recognized in this context the useful contributions of the GGE and the NATO affiliated Cooperative Cyber Defence Centre of Excellence which had produced the Tallinn Manual on the International Law Applicable to Cyber Warfare. He recognized these and other discussions as important 'starting point', but drew attention to some of the inherent difficulties such discussions would inevitably face. According to Dr Melzer many ambiguities can arise when applying existing law to the cyber domain, as the terms of these provisions do not easily fit the characteristics of cyber space as they were originally designed for the physical world. Many ambiguities arise, for example, due to the absence of borders in cyberspace, delayed cause-effect in cyber operations, and non-transparent control patterns which challenge attribution. Additionally, he noted, it remained unclear what the conventional notions of 'force' or 'attack' meant in cyber space, that the distinction between 'civilian' and 'military' objects would be even more difficult, and that it remained unclear what rights and duties would arise from a state's territorial 'sovereignty' or 'jurisdiction'. Relying on an overly technical approach based on the literal application of existing treaty law to cyber, is therefore often inconvertible in practice. Dr Melzer further highlighted the lack of cyber-specific customary rules due to the absence of clearly identifiable state practice and consistent '*opinion juris*' on cyber issues.

One possible way forward would be to look at existing international law through the lens of the long-standing fundamental principles underlying and informing the entire legal framework, he suggested. Instead of discussing whether cyber operations against civilian data and networks can be viewed as a form of 'attack' within the meaning of Article 49 AP I,[7] or discussing whether such data constitutes a protected 'object' within the wording of a treaty drafted at a time when non-physical data was not yet a significant issue, Dr Melzer suggested that it would be more fruitful to refer back to the longstanding and uncontroversial IHL principle which requires the general protection of the civilian population

7 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

during armed conflict. The principle of 'distinction', as enshrined in the Laws of Armed Conflict (LOAC),[8] requires belligerents to distinguish between civilian and military targets and prohibits attacks against civilian persons and objects. According to this principle, sabotage and attacks on civilian data would be impermissible beyond doubt and clearly violate customary law and the general humanitarian purpose of the LOAC. He suggested that similar principle-based approaches might be useful for clarifying the meaning of 'sovereignty', 'armed attack' or 'jurisdiction' in cyberspace.

Dr Melzer emphasized the positive impact of norm-clarification for confidence building and noted that these considerations should come prior to considerations about supposed gaps in the existing legal framework. He stressed the need to find alternative and complementary ways to clarify existing law and to identify and develop new norms and standards for cyberspace. He suggested that a multi-stakeholder approach should be followed, given that key actors in cyberspace include not exclusively states, but also multilateral and regional organizations, business corporations, and private individuals, represented by civil society organizations.

Dr Andrii Paziuk delivered the second presentation on the application of international law in cyberspace in which he focused on lessons learned from history and doctrine. First, he drew attention to the diverse sources of international law, as codified in Article 38 (I) of the Statute of the International Court of Justice (ICJ),[9] which lists not only treaty law, customary law and general principles of law, but also judicial decisions and juristic opinions. Dr Paziuk then identified a number of cases which might offer useful guidance for the discussion on how to address the question of cybersecurity.

In the *Wimbledon* case[10] the Permanent Court of International Justice (P.C.I.J.) had decided that the usage of the Kiel Canal, even though an internal waterway, is free and open to all nations at peace, thus, de facto an international waterway. Dr Paziuk suggested that such international waterways are comparable to transborder data flows and proposed the establishment of an international legal regime for transborder data flows analogous to the regime regulating international waters. He suggested that such a cyber regime would entail freedoms, such as 'free transborder data flows', and responsibilities, such as ensuring that limitations of access and blocking of specific contents would comply with international human rights standards. In this context he stressed that the principle of due diligence would apply, wherefore state policies should identify and avoid interferences with internet traffic.

Recalling the Court's decision in the *S.S. Wimbledon* case he stressed that all states have the right to enter into international engagements and that those may place restrictions upon the exercise of sovereign rights by requiring the contracting state party to exercise its sovereignty in a certain way. In the same vein sovereignty may also be restricted through the imposition of duties and responsibilities in the cyber domain. In this context he stressed, however, that a state's inability to 'prove display' of territorial sovereignty in a certain context would not necessarily mean that sovereign rights would be inexistent.[11] Dr Paziuk referred to the decision of the *Island of Palmas* case from 1928,[12] which acknowledged that gaps, intermittences in time, and discontinuity in space is a common and necessary circumstance and does not imply that sovereignty vanishes. He concluded that the positive

8 1977 Additional Protocol I and II of the 1949 Geneva Conventions.
9 United Nations, *Statute of the International Court of Justice*, 18 April 1946.
10 *S.S. Wimbledon* (U.K. v. Japan), 1923 P.C.I.J. (ser. A) No. 1 (Aug. 17).
11 *Island of Palmas* (Netherlands, USA), 4 April 1928, R.I.A.A., vol. II, p. 855.
12 Ibid.

obligation of a state to protect the right to integrity and inviolability in peace and in war time, and its duty to protect the national rights of its citizens 'in foreign territory'—would also apply to the transborder sphere of cyberspace, even in the absence of effective display of sovereign rights. Further limitations to national sovereignty in cyberspace could be derived from principles of existing international law, such as the 'no harm' principle, which prohibits any activities and usage of their territory in a way which will damage the territory, the properties, or the persons of another state.[13] Besides such "negative" obligations other positive obligations may exist and require states to take necessary steps to ensure that activities within their jurisdiction and control do not cause damage to the environment.[14]

Dr Paziuk emphasized that the establishment of limitations to sovereign rights of states through the creation of obligations under international law is a common and necessary practice to ensure the protection of 'common interests'. He emphasized that the principles of precaution, 'no harm' and 'due diligence' apply in cyberspace and, in this vein noted that the principle of precaution, for example, might require states to take active steps to protect and enhance their citizens' rights in cyberspace. He suggested further that transparent and multi-stakeholder processes should be established to implement and ensure the protection of common interests, emphasizing the importance of universal access, enjoyment of human rights and freedom of innovation.

In the third presentation of this panel, **Dr Zwanenburg** addressed the current legal and policy initiatives related to the application of international law to cyber space. In his preliminary remarks he suggested that most of the existing initiatives could be divided into two categories, namely those that are concerned with the clarification of existing international law, and those that focus on norm development, either by focusing on confidence-building measures (CBMs), or on legally non-binding norms. Dr Zwanenburg stressed, however, the importance of recognizing the blurred line between non-binding 'soft' and binding 'hard' law. In this context he noted that norms that are initially non-binding and voluntary (i.e. rules or principles of responsible state behaviour) may morph into 'hard law' over time, for example, when incorporated into formal treaty law, or by acquiring the status of customary law, identifiable through coherent state practice or 'opinion juris'.

Dr Zwanenburg noted that the consensus on the existence of applicable 'hard law' to cyberspace, in itself, was insufficient to clarify *how* it should be applied given the ambiguities arising from the fact that many norms were created in the past without specifically considering cyberspace. Dr Zwanenburg stressed the need to create a broader consensus on the application of existing law and stressed the importance of a broad and inclusive engagement in the discussion, suggesting that more clarity and transparency in the discussions could, in itself, contribute to more stability in the cyber domain.

Dr Zwanenburg went on to discuss and highlight three initiatives dealing with the application of international law to cyberspace. First, he presented the work of the GGE in the Field of Information and Telecommunications in the Context of International Security. The GGE was established by the United Nations General Assembly and includes the P5 countries (China, France, Russia, the United Kingdom and the United States) and other important state actors in the cyber-domain. The second GGE report of 2012–2013 is, according to Dr Zwanenburg of significance, as it explicitly confirmed the applicability of international law and, in particular, the United Nations Charter. Moreover, by doing so, it recognized the essential role

13 See also *The Trail Smelter case*, USA, Canada, 16 April 1938, 11 March 1941, RIAA, Vol. III, pp. 1905-1965.
14 See also *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports, 1996, p. 226. para. 29.

of international law for the maintenance of peace and stability, and for the promotion of an open, peaceful and accessible Information and Communications Technology (ICT). Therefore, existing international law provides a starting point for the discussions on cybersecurity. He expects further progress through the mandate of the United Nations General Assembly Resolution 68/243 for the GGE 2014–2015, to continue its investigation of how international law applies to the use of ICTs by states. The second initiative presented, was the Tallinn Process which lead to the drafting of the Tallinn Manual on the International Law Applicable to Cyber Warfare, published by the Cooperative Cyber Defence Centre of Excellence. Dr Zwanenburg called it a comprehensive manual focusing especially on the rules applying to the 'use of force'. The Tallinn Manual 2.0 is expected to be finalized in 2016, expanding its focus also on the rules of international law applying in peacetime. The third initiative presented, was UNIDIR's Regional Seminar Series. The particular strength of this initiative, according to Dr Zwanenburg, is its broad engagement with, and the inclusion of different regions into a comprehensive and sustainable dialogue. He contrasted this approach with the one of the GGE, which assembles only a relatively small number of states.

Next, Dr Zwanenburg presented some initiatives which also dealt with norm development. He first noted that some countries had suggested norm development in the GGE. In this context he mentioned a draft Convention on International Information Security to 'limit threats to international information security [and to] ensure the information security of States Parties' proposed by the Russian Federation in 2011. The draft convention proposes establishing an international legal regime regulating military activities in cyberspace through international cooperation. Dr Zwanenburg noted that this proposal was mostly supported by non-Western states, for example, members of organizations such as the Collective Security Treaty Organisation (CSTO), the Commonwealth of Independent States (CIS) and the Shanghai Cooperation Organisation (SCO). Also in 2011, China, Russia, Tajikistan, and Uzbekistan submitted a draft resolution for an international Code of Conduct (CoC) for information security to the UN General Assembly, and, in 2015, together with Kyrgyzstan and Kazakhstan, a revised version of the initial CoC. Other examples for norm-building initiatives mentioned were efforts to establish confidence building measures (CBMs) by the Organization for Security and Co-operation in Europe's (OSCE), and the Association of Southeast Asian Nations (ASEAN) Regional Forum. Lastly Dr Zwanenburg mentioned the 4th Global Conference on Cyberspace (GCCS), held in The Hague in 2015, as a positive example for a forum that brought together a range of actors to discuss key developments in the cyber domain including governments, intergovernmental organizations, the private sector, civil society, academia, and the technical community. It was noted that the conference contributed to the exploration of the development of voluntary, non-legally binding norms for responsible behaviour in cyberspace during conflict and peacetimes, while calling for a broad and inclusive engagement of the international community. A number of events during and in the margins of the conference were devoted to enhance inclusiveness, for example, by giving states the opportunity to discuss the draft chapters of the Tallinn Manual 2.0 with the drafters.

Dr Zwanenburg remarked that the broad emphasis on international law reflected the general view that it was considered an important instrument to ensure peace and security in the context of cyberspace. He concluded by stating that his country, the Netherlands, considers broad engagement and expanded dialogue as vital and, in this context, expressed his compliments to UNIDIR for facilitating such processes through its Regional Seminars.

The subsequent discussion centred on the legal issues surrounding the debate on the applicability of international law to cyberspace. The Law of the Sea were suggested again

as a source of guidance for dealing with the cyber domain in the sense that both the sea and cyberspace are common resources offering economic and cultural benefits for private and state actors alike. At the same time attention was drawn to important differences between the two domains. In this context it was noted that different national security or economic concerns are accounted for by the laws governing the maritime environment as it distinguishes between different zones, such as territorial waters, the High Seas, or Exclusive Economic Zones, which have different implications for sovereign rights and duties. This example was used by the panellists in order to highlight the importance of balancing the common interest of a free and open internet on the one side, and the need to take into account critical state interests on the other. One panellist noted that his balance has been successfully struck in the sea environment, however, the same might be more difficult in the cyber domain. A further major difference between the sea and the cyber environment noted was the fact that the physical infrastructure necessary for conducting data streams is mostly private property. It was also noted that the codification of norms and rules for the sea was a process that was based on state practice and took hundreds of years and involved many actors and stakeholders. It was concluded that the same is necessary for the codification of norms applying to cyberspace. Whilst timeframes may be different, the importance of maximal participation of multiple actors in the discussion on norms and laws for cyberspace was crucial for reaching a common understanding of state practice. In this context, one participant also mentioned the Antarctica regime, which protects a specific global resource, as an alternative way of looking at the protection of cyberspace as a common resource.

Panel 3. The Use of Force

- **Armed Attacks: Legal Thresholds in Cyber Activities**
  Mr Laurent Gisel, Legal Adviser, International Committee of the Red Cross
- **Cyberweapons: A Reality?**
  Ms Alexandra V. Kulikova, Program Coordinator, Global Internet Governance and International Information Security, PIR Center

Panel 3 explored legal and practical dimensions of the use of force in cyberspace. Panellists presented and discussed the difficulties arising from applying conventional terminology of international law in the cyber domain. Major difficulties included the lacking consensus on how to interpret threshold requirements that trigger the application of the Law of Armed Conflict, such as 'use of force' or 'armed attack', and how to qualify and address the disruptive effect of hostile cyber operations below the conventional threshold requirements. In this context the term 'cyberweapon' was problematized.

Mr Gisel focused during his presentation on the question of threshold of the use of force and issues arising from the application of the Laws of Armed Conflict (LOAC) to cyberspace, focusing particularly on the rules of jus in bello. He began by distinguishing between cyber warfare, in which cyber attacks constituted means and methods of warfare, and cyber attacks outside the context of armed conflict. He stated that the ICRC is concerned with novel technologies and cyber in so far as they are potentially used in the context of an armed conflict and, more specifically, with the potential human costs arising from their use as well as the legal implications.

Mr Gisel noted that many of the notions of the jus ad bellum and jus in bello allow for different interpretations as they are not clearly defined by the law itself. He identified two

threshold questions of jus ad bellum, namely the use of force and the notion of armed attack. He noted that the threshold is generally considered to be higher for the latter, but also highlighted the existence of different interpretations. To be distinguished from this general issue regarding the interpretation of threshold are those which are cyber specific. In this context he noted that there was little dispute about the fact that a cyber attack that would fulfil the kinetic effects of a conventional attack would also be considered in the same way. He noted, however, that it was difficult to qualify cyber operations that would lack comparable kinetic effect, for example, 'bloodless' cyber attacks, resulting merely in the loss of functionality without necessarily causing physical damage. He also suggested that it might be more difficult to distinguish between 'attack' and espionage in cyberspace, but noted that economic espionage was generally not considered to qualify as 'use of force'.

In the context of the conduct of hostilities Mr Giesel noted that it would not make a difference whether a computer system was disabled through physical or cyber force as the principles of LOAC prohibit attacks on civilians and civilian objects. He noted, however, that it may be more difficult to distinguish between civilian and military objects in cyber space. One recommendation made by Mr Gisel for the protection of sensitive and vital critical infrastructure was to keep important institutions and records disconnected from the internet, even though this might not offer 'bullet-proof' protection.

Lastly, Mr Gisel stressed the importance of awareness of different interpretations of threshold requirements to avoid unnecessary escalation and therefore highlighted the merit of continued discussions even in the absence of a common understanding. He briefly mentioned, for example, the existence of different views about whether 'kinetic' self-defence was a permissible way to respond to cyber operations.

Ms Alexandra Kulikova began by illustrating the 'realness' of cyberweapons by showing an animated map by 'Norse Dark Intelligence'[15] that visualized the source and the target of over hundred cyber attacks in real time. Ms Kulikova remarked that cyber attacks are precise, and of course dangerous in the context of warfare. She noted, however, that it was impossible to single out any specific technology as 'weapon' in cyberspace, because of the inherent dual-use nature of hard and software. She noted that 'cyberweapon' was a useful metaphor for an implicit threat, but not something that could be 'banned' as such. Ms Kulikova expanded on the difficulties related to the terminology of cyberweapons before she suggested an alternative view on cybersecurity as information security.

She noted that the problem of identifying a cyberweapon is essentially related to the threat of 'aggression', and therefore our understanding thereof. Ms Kulikova offered UN GA resolution 3314[16] as useful clarification of the meaning of 'aggression', but emphasized the absence of a universally agreed interpretation of threshold as well as its lacking guidance on how to qualify malicious use of ICTs as such. In contrast to the GA resolution, she presented the Tallinn Manual's definition of cyberweapons as "cyber means of warfare designed, used or intended to cause either injury or death of people or damage to or destruction of objects". In this sense, Ms Kulikova noted that the identification of cyberweapons was possible only indirectly, by reference to the scale and effect of a cyber attack, but that the wording of the Tallinn manual alone was insufficiently clear for doing so. Ms Kulikova

15 The slide used 'Norse Dark Intelligence' a tool that collects live threat intelligence from 'darknets' in hundreds of locations in over 40 countries in real time.

16 UN General Assembly resolution 3314 (XXIX) of 14 December 1974; Defines aggression in Article I as "the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."

noted that such a definition would compromise software, or viruses, used for intrusion or disruption of critical infrastructures (e.g. military defence systems, communications, electric power smart grids, financial systems, air traffic control etc.). She then suggested additional indicators that have been used to identify cyberweapons in the past, namely the specific technique used, such as secrecy, one-off, deliberative, limited action. Ms Kulikova described three types of 'cyberweapons' with this approach; (1) Direct malicious technologies of selective type (exploiting vulnerabilities, one-off, limited action, no deterrence potential), such as Stuxnet, (2) Intrusion with remote operation (data collection through a long-term exploit, modification of the system's functioning, mutative, intelligence and disruption upon necessity), such as Red October, Flame, Fanny – Equation Group, and (3) autonomous adaptive and self-upgrading systems, such as Suter. She noted that these techniques may be useful to understand the nature and the threat of cyberweapons, but that they do not necessarily help in their definition. It remained unclear, for example, whether Stuxnet should be identified as a weapon, or rather an attack. Arguing for the latter one could say that Stuxnet had no deterrence effect. Similar problems would arise when assessing remote intrusions, i.e. for data collection, where it may be difficult to distinguish between spying and attack. Moreover, these techniques would not be helpful in distinguishing between cyber activity, the use of force, and armed attack. Scale and effect of an attack would not constitute a precise measure. Moreover, she noted, various techniques of coercion, which by themselves may not necessarily amount to the 'use of force', were, in fact, often jointly used. Lastly, she noted, that the criterion of 'immediateness' in the identification of an attack was difficult to apply to cyberspace due the often delayed effects of cyber operations.

Ms Kulikova continued by suggesting an alternative view on cyberweapons in a much broader sense as 'information weapons' as it had been originally suggested by Article 6 of the draft Convention on International Information Security first presented at the meeting of senior international security officials held in Yekaterinburg on 21–22 September 2011. Whist the term 'information weapon' disappeared from the subsequent draft in 2015, it is a useful example expressive of a wider norm-building effort that considers interference with national sovereignty in a broader sense, triggered by interference with its information space. Ms Kulikova mentioned other initiatives supporting such norm-building effort as a first step to scale down the 'cyber race', such as the cyber deal between the United States and Russia (2013), and Russia and China (2015) as well as private initiatives, such as Microsoft's '6 Norms of State Behaviour in Cyberspace'.

Ms Kulikova concluded that there was a desire for 'cyber disarmament' even though there was little will to sign a treaty at this point. She drew attention to the fact that many countries develop cyber capacities and warned that it might be difficult to distinguish between capacity building and cyber militarization. She also warned that non-state actors have relatively easy access to cyber resources and that cyberweapons would likely be used as part of hybrid warfare.

The subsequent discussion focused on the threat of cyber attacks against critical civilian infrastructure. It was noted that vital civilian infrastructure, such as nuclear facilities, enjoyed special protection under IHL, but also that often times it may be difficult to distinguish between civilian and military infrastructure in cyberspace. One participant criticized the common consideration of cybersecurity and cyber attacks as matters between state actors and demanded to take non-state actors more into account, an approach analogous to improvised explosive devices (IEDs). The SCO's Code of Conduct (CoC) was mentioned as a starting point to foster technical-corporation between states to enhance protection of vital infrastructures.

Keynote: The Obligation of Due Diligence: Realities and Requirements

- **Mr Jarmo Sareva,** Director, United Nations Institute for Disarmament Research, UNIDIR

In his keynote speech **Mr Sareva** elaborated on the notions of due diligence and state responsibility in the cyber domain.

Mr Sareva noted that the "due diligence" principle, as it is commonly understood to apply to the cyber domain, requires states to take all appropriate and necessary measures to prevent a risk of harm caused by activities originating in its the cyber domain for a third state, be it physical or not. This arguably entails the obligation to ensure that a legal framework is in place to address and remedy the effects of harmful behaviour outside their jurisdiction. This may also entail the duty to investigate and prosecute crimes, and cooperation, for example, when an affected state has limited technical capacity for doing so itself. Mr Sareva pointed out that, particularly in the cyber domain, malicious activities are likely to have trans-boundary repercussions wherefore a mere focus on domestic effects does not suffice. He warned, however, that the nature of states' obligations in the cyber realm remains far from clear. Mr Sareva acknowledged that a common standard for "due diligence" at the international level may be difficult to conceptualize due to states' different attitudes toward regulation of cyber space. At the same time he cautioned that an overly strict standard may mean the increase of 'intrusive' regulation of cyber space. A standard that would be too weak, on the other hand, might encourage cyber "safe-havens", which he compared to "flags of convenience" in the maritime domain.

Mr Sareva referred to case law in order to clarify the meaning of state responsibility in cyber space. The *Corfu Channel* case affirmed that, under customary international law, states have the obligation to ensure that their territory is not used for acts that unlawfully harm other states,[17] a principle that was restated by the Tallinn Manual explicitly with regard to cyber.[18] Mr Sareva further observed that the *S.S. Lotus* case judgement affirmed the same obligation explicitly for criminal activity[19] and noted that state actors are responsible for the action of non-state actors provided that these activities are under instruction, direction and control of that state. With reference to the cyber attacks on Estonia he noted, however, that legal attribution of such kind might be very difficult in cyber space.

Mr Sareva noted, with reference to the *Teheran Hostages* case, that states do have the responsibility to 'take appropriate steps' in order to prevent harm if it has 'the means at [its] disposal to perform [its] obligations'.[20] Whilst emphasizing that a state is not automatically responsible for wrongful acts originating within their territory, he suggested that states that do not currently have any form of cyber crime legislation potentially violate their positive obligation to take appropriate preventive measures.

Mr Sareva concluded that a state is responsible if it fails its obligation to prevent its territory from being used to commit criminal acts against another state, or if it fails to pursue, arrest, and bring to justice criminals who have conducted cross-border attacks on other states. He

17 *Corfu Channel* (UK v. Albania), 1949 I.C.J., Reports 1949. (April 9). "a state is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people"

18 Rule 5 provides that: "State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."

19 *S.S. Lotus* (France v. Turkey), 1927 P.C.I.J., (ser. A) No. 10 (Sept. 7).

20 *United States Diplomatic and Consular Staff in Tehran* (USA v. Iran), Judgement, 1980 I.C.J., Reports 1980. (May 24).

admitted, however, that challenges might arise when applying such principles *in concreto*, for example regarding the determination of a threshold for 'transboundary harm'. Mr Sareva suggested "negative effects manifesting serious consequences" as possible terminology as it would include also non-physical harm in the cyber domain. Lastly, he stressed the importance of discussing at the international level the minimum level of due diligence a state must carry out in preventing its territory from being used as a base, or indeed perhaps transit point, for malicious cyber-attacks, as being a critical part of a future resilient cyber regime.

Panel 4. Initiatives

- **OSCE**
  Dr Nils Melzer, Senior Adviser, Division for Security Policy, Directorate of Political Affairs, Federal Department of Foreign Affairs, Switzerland
- **UN Overview**
  Mr Ben Baseley-Walker, Programme Lead, Emerging Security Threats Programme, UNIDIR

Panel 4 explored various initiatives on international security aspects of cyberspace and, in this context, presented the work of international and regional initiatives by the UN and the OSCE, particularly focusing on confidence building measures. The role of regional efforts for the development of common understanding and in enhancing multilateral engagement and dialogue was highlighted as key element in fostering cyber stability at the international level.

Dr Melzer presented an overview of the work of the Organization for Security and Co-operation in Europe (OSCE). Thereby, he spoke in proxy of the OSCE, as Switzerland is part of the organization's troika chairmanship.

First, Dr Melzer emphasised the organization's general comprehensive approach to security which encompasses three dimensions; political-military, economic and environmental, and a human dimension, including human rights, the rule of law and democracy. He described the OSCE as the world's largest security organization with a geographical scope from Vancouver to Vladivostok, involving 57 participating and 11 partner states. He noted its active engagement in conflict prevention and resolution, and post-conflict rehabilitation, and described it as a platform for dialogue based on consensus finding. Dr Melzer continued to outline the main principles governing the work of the OSCE as codified upon its foundation in the Helsinki act of 1975. These principles include, for example, sovereign equality, the prohibition on the use of force, peaceful dispute settlement, territorial integrity, the principle of non-intervention, cooperation among states, and respect for human rights law *inter alia*, guiding the relations between participating states. He emphasized the historical importance of the Helsinki process as it offered the rival cold war blocs permanent channels of communication, which led to the first generation of confidence- and security building measures (CBMs). In this context he named the Stockholm Document (1986) and the Vienna Document (1990) as being of particular importance, not only because they were the first security agreements in Europe, but also because they defined verifiable measures aiming to build trust and confidence through transparency and predictability. Most notably, these CBMs included the notification and observation of certain military activities including on-site inspections and evaluation, annual exchanges of military information, and regular dialogue on defence planning.

Dr Melzer noted that the OSCE's considerable experience with the development of CBMs was a key factor in convincing participating states to rely on the organization's know-how also in the area of cyberspace. He noted that, since 2011, cybersecurity has moved to the top of the OSCE's agenda, based on a comprehensive understanding that involves not only issues of cyberterrorism and cybercrime, but essentially all aspects of cybersecurity. The OSCE's Permanent Council established in 2012 an informal working group, which was mandated to elaborate a set of confidence building measures that would enhance transparency, cooperation, predictability and stability between states in cyberspace. This resulted in the adoption of an 'Initial Set of OSCE Confidence Building Measures to Reduce the Risks of Conflict Stemming from the use of Information and Communication Technologies' in 2013. He noted that the OSCE was the first organization to issue a document on CBMs which reflects the willingness of participating states to work together in order to create a more secure and more stable cyber domain.

Dr Melzer suggested that CBMs could be understood to consist of three elements; transparency building measures, measures enhancing international cooperation, and additional commitments by states, which would result in increased stability. He noted that the OSCE's initial set of CBMs comprised a total of 11 of such voluntary measures and continued by providing a brief overview over those CBMs that focus on transparency specifically, for example through information sharing of national views, national policies and strategies. He further emphasized Switzerland's efforts, as OSCE Chair in 2014, to build on the success of this process by implementing the first round of CBMs, supporting negotiations for a second round of CBMs, setting a greater focus on fostering cooperation, and, lastly, facilitating the involvement of non-governmental actors.

Dr Melzer finished his presentation with potential 'take aways' for other regions. He suggested that the OSCE is a positive example that regional organizations can successfully contribute to foster mutual trust and cooperation, and that transparency measures may be a first step to lead to cooperation and, ultimately, stability.

Mr Baseley-Walker's presentation offered an overview of the United Nations' efforts toward a secure and stable cyber domain. He noted that UNIDIR's Regional Seminars on cyber held in the Asia-Pacific and the African regions had confirmed that there is a lot of dynamism at the regional level that has focused on making progress towards specific regional agreements. Mr Baseley-Walker noted, however, that lacking regime coherence between different regional approaches may become a challenge for the creation of a regime at the global level, and that thinking about how to fit regional CBMs together was a critical challenge. He noted in this context that, currently, the international community has still very little understanding of what the commonalities at the regional-national level are, and, that it may be even more difficult to find commonalities between 193 Member States within the UN context.

Next, the presentation addressed in more detail some of the current trends within the multilateral system, particularly focusing on areas for states to get more strongly involved, but also addressing some of the challenges the UN faces as an organization. First, he noted that the activities at the multilateral level are characterized by a lack of focal points and that different institutions, such as the ITU or the GA, have addressed different aspects of cybersecurity. He noted that the biggest challenge consists of reconciling the diverse views on how to secure the cyber domain with a comprehensive multilateral approach, whether this should be done through non-binding CBMs, a comprehensive cyber-treaty, or whether one should address 'cyber' issues as a distinct issue in the first place. He noted that not all actors think that a comprehensive multilateral approach is the right way to go forward.

In this context he noted that, since 2010, Member States of the UN have been regularly providing their views on cybersecurity to the Secretary General who subsequently issued reports in 2013 and 2014. There have been several GGEs on information and telecommunications security, of which those in 2010 and 2013 issued a report. He noted that the GGE was considered the UN initiative on international peace and security in cyber with the highest profile even though but twenty Members States are involved in its work. He further noted that the GGE has merely the status of an advisory group and that its members operate, in theory, in a personal capacity, not national. He explained that there are no other processes or fora where the issue of 'cyber' could easily be introduced and that this reflects, again, the challenge of applying the traditional multilateral architecture to matters of international peace and security in cyber. Whether to consider cyber-issues as 'sub-issues' of other issues, or whether to treat it as separate issue altogether, Mr Baseley-Walker stressed that there are multiple ways to understand cybersecurity. One of such approaches is, for example, to understand cybersecurity as 'cyber stability', or as 'information security', as suggested by the proposal for an international code of conduct (CoC) that had been introduced by members of the Shanghai Corporation Organisation (SCO) to the GGE in 2011.

One other institution that addresses the issue of cyber within the UN framework, Mr Baseley-Walker highlighted, is the International Telecommunications Unit (ITU), which has for a long time been the trailblazer on cybersecurity on the multilateral level. However, the ITU's mandate is mostly of a technical nature rather than a strategic or political one, especially as regards international peace and security. Another example given was the World Conference on International Telecommunication (WCIT) in Dubai (2014), which again evidenced the split between those voices calling for a comprehensive regime approach which also deals with content, and those strongly opposing such a cyber-regime.

In summing up, Mr Baseley-Walker said that the most significant challenge for the United Nations and the international community is to find a common approach on how to conceptualize international security aspects of cyberspace. The next step will be, therefore, to work out what the UN's strategic approach will be and to define what it actually means when talking about cyber and cybersecurity. Furthermore, it has to be explored how the very traditional security structures and approaches within the UN can be adapted to meet some of the challenges, to build confidence, and facilitate dialogue, especially within the regional context, more efficiently. In this context, he recommended to all states to continue to contribute to the reports of the Secretary General and to follow discussions in the UN GA and other UN bodies, so as to broaden the discussion and make as many voices heard as possible on the issue of cyber and international peace and security. In conclusion, Mr Baseley-Walker encouraged strategic reflections on how to fit together national and regional policies.

The discussions following this panel highlighted that clarifying what 'confidence' means in a particular multilateral context was a key element to be taken into consideration when developing respective CBMs. The discussion then focused on the question of whether an instrument like the proposed—and dormant—Code of Conduct on Transnational Corporations[21] is considered to sufficiently regulate data traffic in cyberspace or whether a more cyber-specific code is required. In this context, the growing conflict of jurisdiction between different countries and the challenge of conceiving of cyber in terms of sovereign jurisdictions comparable to territory were mentioned. One panellist stated that this existing

21 See also Draft United Nations Code of Conduct on Transnational Corporations, 23 I.L.M. 626 (1984).

set of parameters would barely amount for transnational cooperation in this sense, lacking inter alia clarity on who is responsible for certain actions. It was concluded that the challenge remains how to conceptualize cyber sovereignty. In this context it was noted that difficulties arising from the effective regulation of the corporate sector was a useful comparison as here it is, similarly, extremely difficult to attribute actions to specific corporate entities and to determine what state has jurisdiction over which activities.

Panel 5. National Views on international Peace & Security Aspects of Cyber

- **Georgia**
  Mr George Jokhadze, Lawyer, Data Exchange Agency, Ministry of Justice, Georgia
- **Oman**
  Dr Nadher Al-Safwani, Cybersecurity Consultant, ITU-ARCC of Oman, Oman

Panel 5 explored national and regional perspectives and approaches to international peace and security in cyber by looking at national policies, safety measures and lessons learned from security implications in the cyber domain. The role of information sharing on national approaches and lessons learned from regional cybersecurity aspects were frequently highlighted as crucial to inform and vitalize the conversation on international law and cybersecurity and to facilitate consensus building on key issues.

Mr Jokhadze focused in his presentation on Georgia's experience with cyber attacks in 2008. He described the cyber attacks as the most clear, and probably only, example of cyber warfare, in spite of the low intensity and physical damage of the cyber-attacks. He noted, however, that the attacks caused extensive disruption of civilian and public services and facilities including the complete disruption of Georgia's communication with the outside world for three days. Attacks on government web resources, media blogs, and the financial sector aimed to cause defacement, manipulation of news reporting, disruption of internet connections and communication networks, and limiting of cash transactions. Mr Jokhadze suggested that the presence of foreign troops on Georgian territory, and evidence collected by international organizations that proved coordination and sources of the attacks, made the attacks attributable.

Mr Jokhadze noted that Georgia was not prepared for such an attack which resulted in a lack of understanding at the political level. Most information on the attacks was in fact provided by outside sources, mostly private organizations. Based on the lessons learned from these attacks, Georgia developed a comprehensive national cyber security strategy in 2011. This strategy comprises a five step approach to enhance research, legislation and the institutional setup, raising awareness of threats and protection measures, and increasing multilateral cooperation, spearheaded by the National Security Council. Laws and regulations on Information Security focused on critical infrastructure protection and include obligations to implement the ISO 27001 standards for Information security management. Furthermore, specific measures on cybercrime were undertaken since 2010 which include the implementation of the 2001 Budapest Convention on cybercrime[22] and the dedication of an investigative unit and expert capacity since 2012. Importantly, separate chapters for cyber issues were established, such as the Data Exchange Agency in the Ministry of Justice,

22 The Convention on Cybercrime, also known as the Budapest Convention, is the first international treaty seeking to address and computer crime. Its main objective is to pursue adoption of legislation and harmonization of criminal policy aimed at the protection of society against cybercrime. It was signed in 2001 and entered into force in 2004.

a Cyber Crime Division with dedicated contact point in the Ministry of the Interior, and a Cyber Security Bureau in the Ministry of Defence. Additionally a State Security and Crisis Management Council under the direct supervision of the Prime-Minister was established in 2014. Mr Jokhadze stressed that the responsibilities of each agency are clearly defined which helps to coordinate their activities.

He continued to present the structure and work of the Data Exchange Agency in more detail. He explained that the Agency consists of an information security division, which is responsible for policy development, implementation and monitoring, and a computer emergency response team (CERT). On a multilateral level, the Agency cooperates with numerous partners including NATO's Science and Peace Project (SPS) and offers free proactive support for incident handling, special services upon request, such as Malware or Source and Binary Code Analysis, as well as training courses on information and cybersecurity for professionals and governmental officials from Afghanistan, Azerbaijan and Macedonia. Mr Jokhadze said that the Agency's Network Monitoring System uses network sensors to analyze real-time net-flow data and to detect anomalies, but emphasized its fully transparent architecture, as defined and required by the law, in order give leverage to Human Rights concerns and to ensure that the Monitoring System is not abused for spying in the private or public sector. Additional measures to improve the safety of the Internet include a safe Domain Name System (DNS) and a black list service and Mr Jokhadze noted that the Agency's response team successfully resolved a number of attacks against Georgian networks and servers.

Mr Jokhadze described Georgia's approach to cybersecurity as a very pragmatic one, one that implemented the lessons learned from the 2008 attacks, focusing especially on critical services and institutions. He noted that Georgia does not distinguish between information and cybersecurity and he highlighted the importance of cooperation also through informal channels as something that has worked very well for Georgia in the past. He also noted Georgia's efforts to integrate the EU regulatory framework on information and cybersecurity (e.g. NIS Directive, ENISA recommendations). At the international level, he noted that it would be more constructive to rely on existing norms, rather than constantly introducing new regulations. Lastly he noted that transparency and information sharing on national measures can help to build trust and that openness on policies would allow others to benefit from them.

Dr Al-Safwani presented the work of the Arab Regional Cybersecurity Center (ARCC), created by the ITU and the Information Technology Agency (ITA) in 2014 as to localize and coordinate cybersecurity initiatives in the Arab region. One of the Center's main objectives is the enhancement of the ITU's Global Cybersecurity Agency (GCA) of 2004 by promoting its implementation within the 22 countries of the region and to develop ideas that can be shared with other regions. He noted that, due to the borderless nature of cyberspace, these efforts would ultimately help to foster global cybersecurity.

Based on GCA's five pillars, ITU-ARCC's services aim for capacity building, international cooperation, development of legal and technical measures, and the establishment of organizational structures. Dr Al-Safwani noted that the different perspectives on cyberspace and cybersecurity among the states of the Arab region were a challenge to the development of a regional approach and that, for this reason, focus on the five pillars was crucial in the development and implementation of national cybersecurity strategies. He further elaborated on ARCC's cybersecurity governance which incorporates ITU's critical national information infrastructure protection (CNIIP) and the child online protection (COP)

guidelines. Cybersecurity assurance and compliance mechanisms include technical services for cybersecurity assessment and implementation as well as audit of Information Security Management Systems. He noted further that the centre aims to enhance incident response through assessment, cyber drills and gap analysis, and noted that the centre offers vital technical and information sharing services. In this context, Dr Al-Safwani listed the numerous activities of the ITU-ARCC which include annual cybersecurity summits and conferences on specific topics. He noted that numerous technical workshops were hosted, for example, on the issue of incident handling, malware analysis, and capacity building in Oman, and on cybersecurity management in Mauretania and Comoros. Additional activities included CERT assessments, two national strategy workshops on child protection in Oman and Bahrain, and specialized training on ethical hacking in Yemen, and on ISMS implementation and hacking in Mauritania. He also noted that the centre organizes cyber drills for governmental officials and encourages through its annual innovation program researchers and experts of cybercrime and cybersecurity to discuss and develop the protection against possible cyber threats. Additionally, the centre raises awareness on cybersecurity issues through the organization of competitions and the awarding of scholarships.

Dr Al-Safwani finished his presentation by stating that the complexity of the centre's work arises from the diverse and innumerable security concerns of cyberspace and reiterated the ITU-ARCC's efforts towards mitigating and preparing for future threats and increasing cyber stability within the region.

The discussion presented different approaches, interpretations and understandings that states and organizations have taken in managing and responding to malicious cyber activities. Also, the discussion highlighted the need for increased cooperation among states, whereby participants emphasized the importance to employ diplomatic and other non-coercive countermeasures against cyber threats first, before resorting to the use of force. Some participants stressed in this context that the definition and the principle of the prohibition of the use of force, in its conventional understanding, may not be sufficient to limit the effects of malicious cyber attacks and its destabilizing effects on international peace and security. Furthermore, the role of private corporations and businesses in assisting the military in carrying out or countering cyber attacks was highlighted, as such activities may transform them into lawful targets under IHL and render them vulnerable even to kinetic attacks. Hence, it was stressed that, besides the states' responsibilities on the issues of cyber stability, the increasing responsibilities of private actors have to be taken into account.

Closing Remarks

In conclusion it was stressed that having an institutional infrastructure in place at the national level may be a critical starting point for the question of how best to address the question of cybersecurity in the context of international peace and security. A focus on the 'reality on the ground' was suggested as a way to shape proprieties. Taking into account the practical aspects of national security, for example dealing with cybercrime and cyberterrorism on a daily basis, may also be important in avoiding an overtly academic discussion of the issues. The continuation of multilateral dialogue was highlighted, once more, as a necessary step to raise awareness about the different conceptions of relevant terminology such as cybersecurity or cyberweapons, and its importance in avoiding that such differences become sources of instability itself. It was recognized that the main focus of the discussion related to the application of IHL to ICTs, but it was noted that there are

numerous other legal bodies, such as investment and commercial law, that may have to be taken into account in the efforts to develop a coherent legal regime. In this context it was noted that it may well be possible that such a regime would be comprised of a set of components that could address different aspects of cybersecurity. It was recognized that there is a long way to go still in this conversation, but it was noted that seminars and regional conferences such as this one are a positive step toward building consensus and enhancing cooperation.

An important message frequently stressed throughout the seminar was the importance of international cooperation and mutual assistance. Both panellists and participants expressed the need for further clarification of existing norms as well as the need to develop norms and guidelines for state behaviour in cyberspace.

UNIDIR

International Law and State Behaviour in Cyberspace Series

Compendium of Regional Seminars

Asia–Pacific Regional Seminar
9–10 December 2014, Seoul, Republic of Korea

Africa Regional Seminar
3–4 March 2015, Nairobi, Republic of Kenya

Eurasia Regional Seminar
3–4 June 2015, Muscat, the Sultanate of Oman