UNIDIR

International Law and State Behaviour in Cyberspace Series

Eurasia Regional Seminar: Conference Report

UNIDIR RESOURCES

Acknowledgements

This meeting is the third in a series of regional meetings in the framework of the UNIDIR project "International Law and State Behaviour in Cyberspace". UNIDIR would like to thank the governments of Germany, the Netherlands and Switzerland for their financial support for this project.

In addition, UNIDIR would like to thank the government of the Sultanate of Oman and the International Telecommunication Union (ITU)—Arab Regional Cybersecurity Center (ARCC) for supporting this regional meeting.

About UNIDIR

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

Note

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

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

The report was drafted by Ralf Gutmann and Elena Finckh.

www.unidir.org

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,[1] 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 during armed

1 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.

conflict. The principle of 'distinction', as enshrined in the Laws of Armed Conflict (LOAC),[2] 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),[3] 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[4] 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.[5] Dr Paziuk referred to the decision of the *Island of Palmas* case from 1928,[6] 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

2 1977 Additional Protocol I and II of the 1949 Geneva Conventions.
3 United Nations, *Statute of the International Court of Justice*, 18 April 1946.
4 *S.S. Wimbledon* (U.K. v. Japan), 1923 P.C.I.J. (ser. A) No. 1 (Aug. 17).
5 *Island of Palmas* (Netherlands, USA), 4 April 1928, R.I.A.A., vol. II, p. 855.
6 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.[7] 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.[8]

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

7 See also *The Trail Smelter case*, USA, Canada, 16 April 1938, 11 March 1941, RIAA, Vol. III, pp. 1905-1965.
8 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'[9] 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[10] 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

9 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.

10 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,[11] a principle that was restated by the Tallinn Manual explicitly with regard to cyber.[12] Mr Sareva further observed that the *S.S. Lotus* case judgement affirmed the same obligation explicitly for criminal activity[13] 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'.[14] 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

11 *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"

12 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."

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

14 *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[15] 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

15 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[16] 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,

16 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

Eurasia Regional Seminar
Conference Report

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

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.