UNIDIR

International Law and State Behaviour in Cyberspace Series

Asia–Pacific Regional Seminar: Conference Report

UNIDIR RESOURCES

Acknowledgements

This meeting is the first 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, the Government of the Republic of Korea generously hosted and supported this regional meeting.

The report was drafted by Daniel Golston.

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

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,[1] 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.

1 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"[2], 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[3] and the Tallinn Manual[4] 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.

2 As described in Article 38 (1)(d) of the Statute of the International Court of Justice.
3 A draft of the International Code of Conduct for Information Security is available at http://nz.chineseembassy.org/eng/zgyw/t858978.htm.
4 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".[5] 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.

5 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.

UNIDIR

International Law and State Behaviour in Cyberspace Series

Asia–Pacific Regional Seminar
Conference Report

9–10 December 2014, Seoul, Republic of Korea

On 9-10 December 2014, the United Nations Institute for Disarmament Research (UNIDIR) carried out the Asia-Pacific Regional Seminar as part of their International Law and State Behaviour in Cyberspace Series. Held in Seoul, Republic of Korea, the Seminar brought together a wide range of government and academic representatives from across the region to discuss some of the key components of international law and its application in the cyber domain.