CONFIDENCE BUILDING MEASURES AND NORMS FOR CYBERSECURITY, AND THE FUTURE OF INTERNET GOVERNANCE

Event Report
3-4 July 2014, Singapore

Centre of Excellence for National Security

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

Event Report

CONFIDENCE BUILDING MEASURES AND NORMS FOR CYBERSECURITY, AND THE FUTURE OF INTERNET GOVERNANCE

Report on the workshop organised by:
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University, Singapore

Supported by:
National Security Coordination Secretariat (NSCS)
Prime Minister's Office, Singapore

Rapporteurs:
Eliane Coates, Joseph Franco, Caitríona H. Heinl, Navhat Nuraniyah,
Senol (Shen) Yilmaz, Jennifer Yang Hui, Yeap Su Yin

Editors:
Damien D. Cheong and Senol (Shen) Yilmaz

The workshop adheres to a variation of the Chatham House Rule. Accordingly, beyond the speakers and presenters cited, no other attributions have been included in this report.

CONTENTS PAGE

EXECUTIVE SUMMARY

Keynote Speech: Cybersecurity 2014: Key Trends and Issues

Irving Lachow kicked off the Workshop by discussing the geopolitical and economic importance of cyberspace. He noted that as most users reside in non-Western countries, this would invariably have ramifications for the future of Internet governance. Lachow also talked about the exponential production and consumption of information, both by humans and Internet-enabled machines. He argued that this would entail revising norms with regard to privacy and confidentiality, which would be further complicated by the growing popularity of "cloud" computing and storage. All these coalesce into a new digital order where power rests with those who control information. In conclusion, Lachow reiterated that in the immediate future, policy will continue to lag behind technological development, while the unpredictability of technological change will continue to complicate policymaking. Thus, the key theme underlying his recommendations was to reconsider the roles held by governments, the industry, and citizens.

Panel 1: Cybersecurity and Cyber-Insecurity: How Serious is the Threat?

The first three panellists provided their insights on strategic cybersecurity issues. David Senty explained that, traditionally, many organisations focus on their own systems to reduce the attack surface with the goal of decreasing cyberthreats. While this is necessary, Senty emphasised the importance of threat based defence and shared his experience from the Advanced Cyber Security Center (ACSC) that is made up of 27 members who share information on cyberthreats for the benefit of all members. Kah Kin Ho, the second speaker, argued that many societies have not found a satisfactory answer to the question of what role governments should play in securing cyberspace vis-à-vis the private sector. Ho suggested a framework consisting of regulatory activities, facilitation to help the private sector to conduct business, and collaboration to meet common goals. Finally, Erik Gartzke opined that emerging (offensive) capabilities in cyberspace are an evolution rather than a revolution in military affairs. Contrary to the view that cyberspace provides a great advantage to hitherto weak actors, Gartzke claimed that cyberspace will prove beneficial to those actors who are already strong.

Panel 2: Emerging Norms for Cyberspace

The second panel focused on "Emerging Norms for Cyberspace". The speakers explored norms in four different realms. Wolff Heintschel von Heinegg's presentation discussed the conclusions from the Tallinn Manual, drawn from legal experts on the applicability of international law in cyberspace. While limited in its approach, the Tallinn Manual nevertheless represented an important first step in identifying applicable international laws. The second speaker, Joy Liddicoat, spoke on human rights norms in cyberspace, advocating a civil society perspective and the building of trust between parties as the way forward. The third speaker, Cormac Callanan, directed attention to regulatory best practices in fighting cybercrime. He stressed the need to build partnerships and cooperation among key stakeholders as a means of dealing with the global and fast changing nature of cyberspace. The last speaker, Irving Lachow, spoke on the current iterations of active cyber defence. He noted that the key word is defence, which is not limited to an offensive move but encapsulates a means of protection that involves active engagement with the adversary.

Panel 3: What Role can Confidence Building Measures play to enhance Cybersecurity?

Panel 3 focused on the role of Confidence Building Measures (CBMs) to enhance cybersecurity. The speakers approached the issue from three different angles: (1) bilateral framework; (2) regional framework; and (3) national strategy, and drew lessons from their respective case studies. Oleg Demidov discussed US-Russian Confidence Building Measures (CBMs) in cybersecurity and highlighted how different countries' conceptual understanding of cyberspace could hamper bilateral cybersecurity CBMs. Ulrich Kuehn noted that

in the European context, the application of traditional CBMs to cyberspace might be limited because unlike CBMs in a traditional setting, CBMs in cyberspace suffer from a puzzling diversity of actors, assets, areas, and accountability. In the case of India's cybersecurity strategy, Cherian Samuel demonstrated how the perceived cyber insecurity has prompted India to reform its national cyber security policy and improve bilateral and multilateral CBMs in cyberspace in order to pursue its goal of a safe and secure cyberspace.

Panel 4: Efforts of International Organisations and NGOs in developing CBMs

The fourth panel focused on "Efforts of International Organisations and NGOs in developing CBMs." Zhang Jing's presentation highlighted China's contribution to international efforts in maintaining security and stability in cyberspace, in particular the country's role in the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). Ben Baseley-Walker noted that Confidence Building Measures (CBMs) play a key role in developing the foundations for progress towards a stable and resilient cyber regime. However its organisation is still a subject of discussion and debate. Daniel Stauffacher shared his views on how civil society may contribute to CBMs in the key areas of (1) transparency and accountability; (2) participation; and (3) deepening the knowledge base.

Panel 5: The Future of Internet Governance

The fifth panel focused on "The Future of Internet Governance". The speakers provided three different perspectives. Ang Peng Hwa presented two different concepts for Internet governance. According to the first, the current form of governance where technical experts agree and make the rules should be continued. Proponents of the second view, however, criticise the lack of legitimation of those involved and favour the involvement of state representatives. The second speaker, John Yong, gave an insight into Singapore's current position on Internet governance covering: accessibility of the Internet; inclusiveness across all segments of society in making use of the Internet; creating a safe Internet space through security layers; and adopting a multi-stakeholder approach to shape a governance framework for the Internet. Noelle de Guzman provided a non-profit organisation's view on Internet governance. She noted that the upcoming ITU Plenipotentiary Conference, where the foundational ITU treaties will be reviewed and possibly revised, might bring the global resource one step closer to possible fragmentation and state control. She opined that more effort is needed to create a governance regime that is flexible and decentralised, and draws upon different stakeholders' common interests.

Panel 6: How to Secure Cyberspace? Three Private Sector Perspectives

The sixth panel focused on private sector perspectives for the securing of cyberspace. Scotland Walsh-Riddle discussed insuring against cyberthreats such as fraud, industrial espionage, and hacking. Given the proliferation of innovations like social networking, cloud computing, and mobile devices, the vulnerability of individuals and businesses has increased. Among other things, he discussed the future for cybersecurity insurance. Bryce Boland shed light on defending critical government networks against advanced attackers. He opined that this requires a threat-centric mindset and a change in security technology acquisition processes. Newer security approaches are more dynamic, identify new or previously unseen attacks, and share intelligence to increase the cost of attack. John Ellis argued that the cloud creates new threat exposures. Security architectures now need to be more data centric rather than network centric. Threats are distributed globally and therefore, policy enforcement should also be global.

Moderated Discussion on Key Takeaways

Wolff Heintschel von Heinegg chaired the moderated discussion and started the session by outlining the three main themes explored during the Workshop: (1) Norms; (2) Confidence-building Measures (CBMs); and (3) Internet governance. For norms, he posed questions on the actual feasibility of achieving consensus. He also highlighted the challenges faced in promoting human rights-based norms and balancing the imperatives

of individual freedoms online and cybersecurity. Regarding CBMs, von Heinegg asked participants whether focusing on procedural aspects would be sufficient. For the area of Internet governance, the push for multi-stakeholder approaches seemed evident in all presentations made during the two-day Workshop. Nonetheless, he pointed out that it is difficult to identify who is a legitimate stakeholder and raised caution in assessing the motives of "self-appointed" guardians of "Internet freedom". In conclusion, von Heinegg remarked that cybersecurity remains conceptually broad, with the increasing reliance on cyberspace met with only limited consideration for national security.

OPENING REMARKS

Opening Remarks
Kumar Ramakrishna, Head, Centre of Excellence for National Security, RSIS

Kumar Ramakrishna

Kumar Ramakrishna observed that in recent times, cyber-threats had surpassed transnational terrorism as the primary challenge to national security in several countries. Current discussions and debates seemed to produce more questions than answers. In light of this, the workshop was organised to firstly, keep abreast of current and emerging challenges in cyberspace, and secondly, glean insights into what could be done to mitigate such challenges.

The workshop had three main themes. The first was Confidence Building Measures (CBMs). Since the open nature of cyberspace facilitates nefarious and destructive actions by various parties, Confidence Building Measures was one instrument to cope with threats from state actors. In the past, arms control mechanisms were employed to manage the threat of nuclear and conventional war. However, since the development and trade of cyber-arms can be carried out in clandestine fashion, monitoring such activities is near impossible. Given these difficulties, perhaps the next best thing is to invest in CBMs to try to reduce the threat of cyber-conflict. The idea being that only through the exchange of ideas, only through getting to know the interests and fears of different parties, would we be able to build mutual empathy and confidence.

The second theme was that of norms that could potentially be applied to cyberspace to enhance cybersecurity. While some groups of states have agreed on sets of laws that are binding internationally vis-à-vis cyber-crime, there are also a number of areas where there is no or little agreement on how laws are applicable, or whether traditional laws can apply, to cyberspace. Some argue that entirely new laws are needed for cyberspace. The workshop was intended to create an opportunity for discussion of these issues.

The third theme that was explored was Internet governance. Many states seem to agree that the current form of governance, exercised by technical experts under the alleged influence of some states, is untenable. However, it remains unclear what the alternatives look like. As such, several panellists will present how they think the future of Internet governance will look like, and more importantly, suggest potential ways forward.

The workshop programme would include: (a) A keynote speech on Key Trends and Issues; (b) Six panels on: (i) cybersecurity and cyber-insecurity; (ii) emerging norms for cyberspace; (iii) what role confidence building measures can play to enhance cybersecurity; (iv) efforts of international organisations and NGOs in developing CBMs; (v) the future of internet governance; and

(vi) how to secure cyberspace; and (c) A moderated discussion on the highlights and key issues emerging from the workshop.

In closing, Ramakrishna encouraged the participants to engage with the speakers, and wished them a stimulating workshop.

Rapporteur: Senol (Shen) Yilmaz

KEYNOTE SPEECH

Cybersecurity 2014: Key Trends and Issues
Irving Lachow, Principal Cyber Security Engineer, The MITRE Corporation

Irving Lachow

Irving Lachow began his presentation by highlighting four important factors pertaining to the current state of cyber-affairs. First, ever since the Stuxnet attacks on Estonia, it has been widely acknowledged that cyberspace has a geopolitical dimension. Second, cyber-technologies are increasingly driving economic growth. Third, cyber-technologies are inherently dual-use. Finally, there were no accepted "rules of the road" for behaviour in cyberspace.

Lachow emphasised that cyberspace is not a purely technical construct, but a man-made one where people matter. Understanding the technological foundations of cyberspace is nonetheless indispensable in resolving the political, diplomatic, military, and economic challenges emanating from societies' reliance on cyberspace.

Cyberspace continues to be in flux, reflecting the shifting demographics of individuals and communities online. It is becoming less Western as Internet usage continues to increase in Asia and Africa. Since non-Westerners will make up the majority of users, they will invariably demand that the Internet be governed according to norms and values that reflect their interests.

Another key trend is the exponential production and consumption of information—not just by humans, but devices comprising the "Internet of Things". Big data analytics is going to become more important in the coming years in terms of volume, velocity and variety. This, Lachow argued, increases the necessity of revising norms on privacy and confidentiality, specifically in light of increasing use of online, cloud-based computing and data storage. Recent events such as the tensions in Crimea demonstrate how control of information and cyberspace translates into power. Asymmetric warfare on the ground was played out in cyberspace as belligerents struggle to ensure: (a) access to information, (b) the integrity of information, and (c) control of the narrative. Cyber-technology, in this respect, plays a key role by providing both the communications infrastructure and social media platforms.

In light of these developments, Lachow observed that: First, policy will continue to lag behind technology. Citing the experience of crafting agreements such as the Chemical Weapons Convention, he pointed out how such processes can take years if not decades. Second, technological change is rapid, accelerating, and unpredictable. Lachow cited how just decades ago, futures thinkers grossly underestimated the market for personal computers.

In addition, as information consumed and produced had become personalised and globalised at the same time, it was likely that an erosion of confidentiality would occur. Furthermore, the blurring between

legitimate and illegitimate activities online would persist. For example, it was hard to distinguish fraud protection from "spying" as well as predictive analytics from "profiling".

In the context of cyber-conflict, Lachow suggested that focusing on the effects/consequences of attacks is more important than the availability of weapons. In terms of developing norms, he also recommended choosing areas where norms could be developed mutually, such as listing vital civilian services and infrastructures as illegitimate targets for cyber-attacks. Lachow also called for a recalibration of the roles of governments, industry, and citizens. Finally, he reminded participants that as much as stakeholders are wary of the threats posed by cyber-insecurity, they should not forget about the benefits of a more connected world.

Discussion

In light of the shift in demographics of global Internet users, a participant asked how countries could be incentivised to create more encompassing norms. A speaker argued that rather than viewing cybersecurity as a zero-sum and adversarial contest, e.g. China vs. the US, states should focus on collaboration. In this regard, other countries in Asia such as Singapore and Indonesia could play a more constructive role to reduce the perceived gaps between East and West.

Another participant inquired about the seeming fragmentation of American efforts to advocate cybersecurity policy, which was observable in the example of the US Department of Commerce and State Department. Lachow acknowledged the existence of these sub-optimal arrangements but also pointed out that institutional dysfunctions were common in other countries as well.

Rapporteur: Joseph Franco

PANEL 1:

CYBERSECURITY AND CYBER-INSECURITY: HOW SERIOUS IS THE THREAT?

A (Technical) Introduction to Cyber-Insecurity for Policymakers

David Senty, Director, Cyber Operations, The MITRE Corporation

David Senty

David Senty provided an introduction to the nature of cyber-insecurity, and explained that in order for defence to be strong, information sharing is critical.

According to Senty, traditionally, many organisations focus on their own systems to reduce the attack surface with the goal of decreasing cyber-threats. This inward looking approach has merits. However, scanning and patching will not be sufficient to guard against sophisticated threats. It is especially difficult to identify assets and vulnerabilities of corporate networks as they are too large and complex. Therefore, Senty claimed that a new approach is needed: Corporations must move away from static defence to threat-based cyber-defence, which balances mitigation with detection and response. An important part of this new approach is that defenders need to become both sophisticated consumers and producers of cyber-intelligence. When threat information is shared with a community, every member can improve their security. However, a precondition is that organisations must become more comfortable with sharing and using threat information. Standards-based threat information repositories are an important first step to ensure that information is communicated and processed quickly. In this context, Senty shared his experience from the Advanced Cyber Security Center (ACSC).

ACSC is a cross-sector regional collaboration in New England between industry, university, and government entities organised to address the most critical cybersecurity challenges. The main objectives of the Center are cyber-threat information sharing, research and development, education, and cyber-policy development. The premise for establishing the Center was the need for protection of intellectual property, cross-sector/interdisciplinary information-sharing, and the alignment of research with operational problems. Today, the ACSC has 27 members that are active in the following industries: defence, financial services, government, healthcare, legal, technology, university, and biotech/pharmaceutical. The members interact in several ways including face-to-face bi-weekly meetings of cyber-defenders as well as bi-monthly meetings of senior leaders. At the same time, members make use of virtual platforms such as a wiki-type webpage and an online forum.

Finally, Senty summarised the lessons learned through the process of establishing the ACSC. Firstly, building networks of trust is crucial since people share information and use information provided by others *only* if there is mutual trust among the members. Secondly, one actor must assume the role of coalition builder and rainmaker. In this context, Senty noted that the government is not likely to succeed in enforcing cooperation but may well act as an initiator of such information-sharing initiatives. Thirdly, for a project such as the ACSC to succeed, several members need to lead by example since some parties may be hesitant at the initial stage. Fourth, a partner entity that is trusted and technologically capable is needed to provide the information sharing infrastructure. Finally, the initiator of such an initiative needs to be patient, especially at the outset as members and/or potential members are reluctant to participate actively.

Strategic Threats and the Way Out

Kah Kin Ho, Head of Strategic Security, Corporate Technology Group, Cisco Systems

Kah Kin Ho

Kah Kin Ho provided a framework for government-private sector cooperation to increase cybersecurity in his presentation. He observed that there is a growing gap in the security capabilities of large enterprises on the one hand and small and medium sized companies on the other. While large enterprises are gaining ground relative to evolving threats, small and medium sized companies' capabilities are decreasing relative to emerging threats. Unsurprisingly, in 2012, large enterprises spent on average USD 591 per employee, whereas small companies spent on average merely USD 61 per employee.

An emerging challenge in this context is that critical infrastructure is owned and operated by private companies. This suggests that closer collaboration between governments and the private sector is needed. The challenge is that governments and the private sector have divergent interests. It is governments' task to ensure national security while maintaining or creating an environment conducive for economic activity. The private sector's main objective, however, is to make profits and serve shareholder interests. In terms of security, it does what it deems sufficient, which may not necessarily be enough. At times, every extra dollar spent on security is seen as decreasing corporate efficiency and shareholder value in the short-term. In the context of Confidence Building Measures (CBMs), Ho also pointed out the paradox between means and interests. Often, while governments have an interest in further developing CBMs, they do not necessarily have the means to do so, the private sector often has the means to enhance CBMs, but it may not have the interest to do so.

Arguably, many societies have not found a solution to what role the government should play vis-à-vis the private sector. Ho opined that a "do as I say" relationship where the government regulates the private sector will be part of the solution, but ultimately, this will be insufficient. In addition to regulation, governments need to ask how they can facilitate the work of the private sector and how the two sectors can collaborate to accomplish mutual goals.

Finally, Ho touched on the issues of cyber-crime and cyber-war. He opined that attribution is possible in selected cases. Cyber-criminals make mistakes in their operations, leaving traces that can be used to identify them. Moreover, only certain parts of a cyber-crime operation actually take place online; cyber-criminals still depend on physical infrastructure in the real world, such as ATMs. On cyber-war, Ho argued that states should build up resilience to be able to withstand minor attacks, and continue to function normally. After all, under international law, not all uses of force amount to an armed attack, and only those that constitute an armed attack would give the victim state the right to self-defence.

The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth

Erik Gartzke, Professor, Dept. of Political Science, University of California, San Diego and Professor of Government, University of Essex

Erik Gartzke

Erik Gartzke argued that some theorists conflate the possible with the actual. In other words, just because

potentially catastrophic attacks are technically feasible, it does not mean that such attacks will be carried out, especially when political and strategic calculations are factored in. The main implication is that capabilities in cyberspace are not a substitute for existing military capabilities but a complement. Therefore, cyber-capabilities will prove most effective for those states/non-state actors that have effective traditional war fighting capabilities. Conversely, they will provide few advantages for weaker entities.

Gartzke observed that cyber-war is often described as the most recent incarnation of the revolution in military affairs. Some theorists have even argued that this transformation of technology and doctrine is capable of overturning the prevailing world order. In Gartzke's opinion, what could happen in cyberspace (or anywhere else) makes little sense without considering how conflict over the Internet is going to realise objectives commonly addressed by terrestrial war. Rather than a revolution in military affairs, he suggested that an *evolution* of military affairs could occur in cyberspace, since cyber-war is not capable of furthering the political ends to which force/threats are commonly applied. Cyber-war is more likely to serve as an adjunct to and not as a substitute for, existing forms of terrestrial force. Rather than threatening existing political or economic hierarchies, cyber-war will likely augment the military advantages of existing major powers.

In support of this argument, Gartzke discussed the theory of war in relation to the cyber-domain. According to military strategist Carl von Clausewitz, war is friction designed to achieve political ends that cannot be achieved in other ways. It is not just noisy and confusing, but informative. States fight to take property or prerogatives from others, or to prevent others from appropriating themselves. The problem with advanced cyber-capabilities is that they are not credible, since anyone could claim to be able to carry out a cyber-attack. However, the opponents are unlikely to believe such threats without evidence. Revealing evidence of a potential cyber-attack degrades military effectiveness. Similarly, cyber-war cannot replace conquest. A cyber-attack can cause damage, but that damage is likely to create only a temporary window of opportunity that must be exploited by other domains (air/land/sea). In conclusion, Gartzke remarked that rather than replacing terrestrial warfare, cyber-war reinforces existing conventional military advantages.

Discussion

A participant wanted to know how governments could incentivise the private sector to work towards enhancing cybersecurity.

A speaker responded that first of all, the government needs to realise that the private sector has a role to play in the context of norm development and cybersecurity CBMs. In neither the United Nations' nor the OSCE's efforts were private sector representatives involved. Furthermore, the speaker opined that the private sector already has incentives to make cyberspace more secure. He noted that pictures were leaked, showing that the NSA had implanted spying technology in a hardware producer's router. This by itself undermines trust. Finally, the speaker noted that tier 1 Internet Service Providers have data that could help in developing CBMs, but this information is not used.

To the question of the possibility of cyber-terrorism, a speaker responded that terrorists may use cyber-technologies to carry out attacks in the future. However, he noted that cyber-attacks are unlikely to cause as much human suffering as traditional attacks, and may therefore be deemed less effective in achieving terrorists' goal of creating visual effects.

Rapporteur: Senol (Shen) Yilmaz

PANEL 2:

EMERGING NORMS FOR CYBERSPACE

The Tallinn Manual: The Laws of Cyberwar

Wolff Heintschel von Heinegg, Professor, Public Law, Europa University Viadrina Frankfurt

Wolff Heintschel von Heinegg

Wolff Heintschel von Heinegg's presentation primarily discussed the Tallinn Manual, which deals with the applicability of international law to cyberspace. The Manual, written by an international group of experts, contains the black letter rules of international law applicable to war as well as how such rules apply to conflict in cyberspace. The experts arrived at the interpretation of the laws by consensus. The experts also included a commentary section, which reflected the different positions taken within the group on the interpretation of the black letter rules with regard to cyberspace. Von Heinegg focussed on two key issues: areas of contention and the right to self-defence in response to a cyber-attack.

First, while there is consensus on the basic premise that international law applies in the cyber-realm, there is also strong acknowledgement of the need to modify and adapt a number of existing laws to make them relevant in the new domain. That states also aim to project power in cyberspace, impacts issues concerning security as well. Some of the main areas of contention in the manual involve issues of sovereignty, state responsibility, *jus ad bellum*, *jus in bello*, occupation laws as well as neutrality and zones. A main area of contestation concerns whether a cyber-operation may violate the prohibition of the use of force under Article 2(4) of the Charter of the United Nations. In this regard, the experts focused on considerations surrounding the definition of 'force', and whether this is limited to kinetic force. Von Heinegg explained that the use of force prohibition has never been limited to kinetic force so that actions in cyberspace may be considered as use of force.

Second, in addressing the right of self-defence, von Heinegg explained that this presupposes a situation of an armed attack or an imminent armed attack. In such cases, a party invoking a right of self-defence is not limited to responding via a cyber-operation but could also resort to the use of a traditional kinetic response. In the context of cyberspace, the key issue revolves around when a cyber-operation amounts to an "armed attack". An "armed attack" is a legal term of art, which according to the International Court of Justice, goes beyond the use of force in terms of intensity. Therefore, an armed attack is an action that causes more damage than a use of force. To distinguish between the two, the scale and effect involved must be taken into consideration. This implies: (a) The effect of a cyber-operation must materialise in the real world and cannot be limited to cyberspace; and (b) to qualify as an armed attack under international law, the scale and affects of the damage would need to reach a certain level. Only then would a victim state be entitled to exercise self-defence. In other words, if a cyber-attack does not reach the degree of an armed attack but is only considered a lower level of a use of force, the victim state would not have the right to self-defence.

In his concluding remarks, von Heinegg noted that the Tallinn Manual is very limited in its approach but is a first important step in identifying the applicable international laws to cyber-operations. The experts did not suggest new laws but rather focused on those laws that are well-established, even though the respective interpretation of the laws may differ. While the Tallinn Manual provides an important snapshot of the existing legal regime, the laws concerning conflict in or through cyberspace may develop very differently in the future.

How do Human Rights apply to Cyberspace?
Joy Liddicoat, Human Rights Specialist, Association for Progressive Communications

Joy Liddicoat

Joy Liddicoat presented on a civil society organisation's perspective on cybersecurity. Some of the challenges faced by a civil society organisation from both state as well as non-state actors include: Internet shutdowns, "just in time" take-down of websites, large-scale surveillance, legal bans on encryption, the banning of anonymity or the use of pseudonyms online and the increasing risk of detention of journalists and bloggers. Another interesting development is the increasing privatisation of policing, with Internet intermediaries taking on the role of content and network policing.

Often, prevailing security measures such as shutting down Internet access causes more panic among the general population rather than achieving the intended objectives of controlling the situation. Hence, human rights conventions and norms need to be considered in measures taken to secure cyberspace, and deliberations between the relevant stakeholders are needed to achieve this. The pace of reforms in this area has not progressed quickly. Moreover, such discussions between states and civil society may be difficult to initiate. They may also be hampered by the profound lack of trust between the two.

In terms of cybersecurity, governments have, by virtue, a right and a major role in securing cyberspace in the interest of public order and national security. The main question to be considered is whether governments can achieve this in a way that is consistent with their international human rights obligations. In 2012, the United Nations Human Rights Council (UNHCR) adopted a resolution for the protection of human rights on the Internet. The basic premise was that the same human rights available offline must also be protected online. Furthermore, the resolution called upon states to promote and facilitate access to the Internet in recognition of its global and open nature in facilitating better interactions. More than forty nations have signed on to the resolution.

As such, there has been a noticeable increase in discussions concerning human rights norms on the Internet; however, there is still a lack of jurisprudence covering this area. To address this, a number of civil society organisations have collaborated with legal experts and produced a list of thirteen legal pronouncements referred to as the *Necessity and Proportionality* principles. Over three hundred organisations have stated their support of these principles, which have also been adopted by a number of political parties.

In conclusion, Liddicoat acknowledged the mutual security concerns that governments and civil society have in cyberspace. While governments have legitimate reasons for concerns over threats to cybersecurity, these concerns are shared by the private sector as well as civil society. An important step is to open the doors for civil society participation in cybersecurity policy-making.

Regulatory Best Practices to fight Cyber-crime
Cormac Callanan, Owner/Founder, Aconite Internet Solutions


Cormac Callanan

Cormac Callanan's presentation discussed several regulatory best practices to fight cyber-crime. He

discussed: (a) the challenges faced by the police in fighting cyber-crime; (b) several European initiatives; and (c) what is needed to encourage more collaboration to fight cyber-crime beyond international borders.

In an increasingly complex cyber-landscape, governments and national enforcement agencies face mounting challenges of operating in a fast changing, international environment. Crimes such as child pornography, identity fraud and theft, are often carried out through the use of dual-use technology. As such, they pose difficult challenges for collaborative efforts amongst law enforcement agencies across countries. At present, law enforcement personnel from different jurisdictions cooperate through Mutual Legal Assistance Treaties (MLAT). However, in practice, collaboration under the MLAT framework causes much delay in carrying out investigations. Investigators are also confronted with a growing number of cyber-crime cases, increasing complexity, reduced resources as well as upskilling challenges. Moreover, national priorities often take precedence, and as such, governments need to come to a consensus on certain core issues concerning cyber-crimes.

In the European context, there are three key agencies working on cyber-crime. The European Cybercrime Centre (EC3) deals with cyber-crime, the European Network and Information Security Agency (ENISA) deals with general cyber-security issues and the European Police College (CEPOL) provides training for law enforcement personnel. The European Commission has set up the European Cybercrime Task Force which brings together the heads of European Union cyber-crime units to facilitate the cross-border fight against cyber-crime. A Cybercrime Centres of Excellence network has also been established to enable joint initiatives to train law enforcement personnel. The Organisation for Security and Co-operation in Europe (OSCE) for example, has projects related to confidence building measures in a number of Eastern European countries.

To build more effective collaborative models, Callanan urged law enforcement to build partnerships with those in academia and those who work in IT in the private sector. Access is needed to key engineers in such industries in order to facilitate hands-on training of law enforcement officers. Another area in which partnerships should be built is between law enforcement, prosecutors and the judiciary to enable the creation of an investigative and legal system with capabilities to investigate, charge, and prosecute cyber-crimes in an effective manner. One area that should not be neglected is the provision of guidelines on the ways in which different entities collaborate with each other, in sharing, training and conducting relevant research.

In conclusion, Callanan argued that law enforcement agencies would undoubtedly be confronted by a wide range of new challenges in cyberspace including virtualisation, mobile technology and cloud computing.

Active Cyber Defence

Irving Lachow, Principal Cyber Security Engineer, The MITRE Corporation

Irving Lachow

Irving Lachow's presentation discussed policy and strategy considerations for active cyber-defence (ACD). He began by noting that the key word to be considered is defence, which indicates that the actions involved are defensive in nature. As such, ACD does not connote reciprocal hacking or cyber-operations with a purely offensive motive. Rather, it involves active engagement with a cyber-adversary. There is increasing interest in this area given that the rate of cyber-crime is rapidly growing while the ability of law enforcement to respond is limited. To address this, businesses have been considering ACD capabilities as a possible approach to network breaches as opposed to more passive attitudes.

There are a number of major challenges for organisations interested in employing ACD. First, there is no universal definition of ACD. Second, the parties are faced with a

conundrum since tensions arise between what is legally permissible and what is technologically possible. Third, the roles of governments and the private sector are not clearly demarcated, especially on issues concerning actions that can be taken by companies and individuals, and how far they can go. At present, there is no single analytical framework that captures all the dynamics and issues at hand.

In terms of legislation for example, the Computer Fraud and Abuse Act (CFAA) in the United States is the main regulatory framework for cybersecurity. However, many of the provisions of the act exclude a large number of ACD options. For example, the act states that it is illegal to exceed authorised access on a "protected computer". This includes computers located outside of the United States. Moreover, there are mixed views as to whether the CFAA is too strict or too lenient in terms of the possibility of engaging in ACD actions.

Another framework of analysis involves the law of armed conflict. This body of law does not directly apply to actions that can be considered ACD. Other legal concepts that have been applied include the right to self-defence, hot pursuit and carrying out a citizen's arrest. Lachow noted that the latter provides a compelling framework for ACD but the use of force in this instance has to be proportionate to the act being committed.

From a purely legal perspective, there seems to be many grey areas in addressing options for ACD. However, there may be much at stake in trying to prevent cyber-attacks despite the growing number of questions being asked over the legality of actions. Another possible angle for analysing ACD options takes into consideration four main features: (a) the scope of the effects; (b) the degree of cooperation; (c) types of effects; and (d) how automated the response is. However, Lachow observed that merely considering the legal aspects of ACD is not sufficient as this precludes the wider societal costs and benefits involved.

Discussion

A participant inquired about the possibility of balancing law enforcement needs with a human rights perspective. A speaker replied that the perception that law enforcement would inevitably breach human rights norms while pursuing cyber-criminals is erroneous. On the contrary, law enforcement agencies play the role of human rights defenders, carrying out the obligations of states in protecting their citizens.

A question was raised regarding how human rights organisations viewed the role of private companies, such as Facebook, in privacy protection especially since they possess large databases of private information. A speaker replied that businesses have traditionally not considered themselves parties to human rights debates but many increasingly see this as an untenable position with the possibility of negatively impacting the conduct of their operations.

A question was raised regarding the second installation of the Tallinn Manual (Tallinn 2.0). A speaker replied that this was still work-in-progress, and would encompass other international legal issues that have not been addressed in the first Manual.

A participant inquired as to whether there were ways to encourage the participation of other countries in the development of the Tallinn Manual, given that only experts from NATO member countries were invited. Broad participation, the participant argued, may ensure broader acceptance. A speaker replied that there have been other manuals which are similar to the Tallinn Manual such as the San Remo manual on the law of naval warfare. These are compilations of expert opinions on the state of the law. While predominantly academic in character, these manuals have, nevertheless, had tremendous impact on the development of the law in many states.

Rapporteur: Yeap Su Yin

PANEL 3:

WHAT ROLE CAN CONFIDENCE BUILDING MEASURES PLAY TO ENHANCE CYBERSECURITY?

United States-Russia Confidence Building Measures in Cyberspace: Backgrounds, Advantages, and Failures

Oleg Demidov, Program Director, The Russian Center for Policy Studies

Oleg Demidov presented on some of the key challenges as well as achievements in US-Russia Confidence Building Measures (CBMs) in cybersecurity. An embryonic bilateral initiative on CBMs in cyberspace was initiated in the 1998 US-Russia Presidents' Joint Statement on "The Common Security Challenges at the Threshold of the 21st Century", which called for "resolving the potential Year 2000 computer problem" among other issues.

In 2012, official agreements on practical bilateral cooperation in cybersecurity were drafted, but the formal agreements were not signed until 2013. The stalemate occurred largely due to a terminological dispute, namely between the term "cybersecurity", which the US favoured, and "international information security", as preferred by Russia. The US understanding of cyberspace specifically refers to the global domain of the information environment including the Internet, telecommunication systems, and computer networks. Whereas Russia prefers a definition of information space that is broader in scope and includes any activity related to the creation, transfer, use, and storage of information that could have social and political impacts. As such, Russia prefers including content-related issues as well. Demidov argued that the terminological dispute actually represents a long-standing conceptual gap between US and Russian understanding of cyberspace.

Despite the initial hurdle, US-Russia bilateral agreements on cyberspace CBMs have yielded some practical results, such as the active exchange of information on cyber-threats before and during the Sochi Olympics; the establishment of a direct communication link between high-level officials in the White House and the Kremlin; the establishment of a communication channel and information sharing arrangements between computer emergency response teams (CERTs) of the USA and Russia; and the inaugural meeting of the Working Group on Threats to and in the Use of ICTs in the Context of International Security. Furthermore, the bilateral cooperation in cybersecurity was not affected even when Russia granted asylum to Edward Snowden.

Demidov observed that the US-Russia bilateral agreement did have operational challenges. First of all, it was not inclusive enough in terms of issue coverage. The agreement, for instance, did not enable cooperation in critical information infrastructure protection. Secondly, the consensus on terminology was reached only through sweeping the differing Information and Communication Technology (ICT) security paradigms under the rug rather than resolving it. Expectedly, this could lead to disputes in the future. Finally, the implementation of the agreement still hinges on the general quality of bilateral relations. For example, the deteriorating bilateral relationship between the US and Russia in light of the Ukrainian crisis has halted the implementation of the agreement. In other words, the bilateral CBMs on cybersecurity are still vulnerable to turbulences in the bilateral relationship.

In sum, Demidov noted that although US-Russia bilateral CBMs in cyberspace have encountered significant challenges, the process has nevertheless provided valuable lessons learned for other bilateral and regional frameworks. For instance, they underscore the importance of resolving differing ICT security paradigms as well as the necessity of establishing practical measures and direct communication links. They also provide a potential blueprint for regional cyberspace CBMs.

Applying Insights Gained from Traditional TCBMs to Cyberspace

Ulrich Kuehn, Researcher, Institute for Peace Research and Security Policy, University of Hamburg

Ulrich Kuehn

In his presentation "Applying Insights Gained from Traditional TCBMs to Cyberspace", Ulrich Kuehn focused on two main points: (1) the lessons learned from traditional military Transparency and Confidence Building Measures (TCBMs) in the European context; and (2) the potential applicability of traditional military TCBMs to cyberspace and the challenges of doing so.

Kuehn began his talk by presenting four lessons learned from traditional TCBMs in the European context. These were premised on his observations of traditional military TCBMs in the context of the Commission on Security and Cooperation in Europe (CSCE) as well as in the Organization for Security and Co-operation in Europe (OSCE). First, in terms of institutionalisation, successful formation of TCBM regimes does not necessarily guarantee peaceful conduct. In fact, a security regime can erode overtime if it fails to agree on timely measures that promise equivalent gains to the member states. Secondly, on the issue of norms and principles, he suggested that the more open the formulation, the easier to agree on a working agenda. However, once such principles and norms are agreed upon, they would be hard to change. Such a tendency of norm hardening could be a challenge to cybersecurity cooperation as the relevant technology changes rapidly in cyberspace. Thirdly, in regard to working agenda and treaty implementation, politically binding agreements are easier to establish as opposed to legally binding ones. Learning effects could lead to continued implementation of such agreements even in times of crisis. Finally, Kuehn observed that even legally binding agreements cannot always prevent non-compliance, especially when states' vital interests are at stake.

As far as the potential applicability of traditional military TCBMs to cyberspace is concerned, Kuehn opined that due to the unique nature of cyberspace, this may be difficult. Compared to traditional military cooperation, cybersecurity cooperation is more challenging as it suffers from a lack of clear definition and the puzzling diversity of four factors: actors, assets, areas, and accountability. First, actors in cyberspace include states, NGOs, private businesses, and individuals. The multitude of actors means that concluding CBMs with all actors is very unlikely. Second, unlike traditional military cooperation whereby the assets are relatively distinguishable, almost all assets that could be used for a cyber-attack are of a dual-use character, cheap and easily accessible. A clear distinction as to what assets are meant purely for military use is difficult to ascertain. Transparency and verification measures in cyberspace would need extremely high willingness to be transparent among a multitude of actors. Third, areas in traditional military TCBMs are defined by geographical borders. It may therefore be possible to apply transparency measures in specific geographical areas of heightened tension. Generally, however, "area" would require a totally new definition. One suggestion would be to focus on specific key installations such as nuclear installations, stock exchanges, undersea cables, etc. Finally, accountability and verification of compliance is also much more difficult in cyberspace due to the multitude of actors and the possibility of concealing one's identity in cyberspace.

Considering the different characteristics between traditional military TCBMs and TCBMs in the context of cybersecurity, a lesson learned from the European TCBM efforts is that maintaining the political process of cooperation may be more useful than a specific operational document. Bearing this lesson in mind, the OSCE recently experienced a progress in its effort to build international governance of cyberspace with the release of OSCE Permanent Council Decision No. 1106 (3 December 2013) which, among other things, calls for voluntary exchange of national views and information on cybersecurity, and for voluntarily provision of a list of national terminology in order to solve the terminological gap.

India's International Cybersecurity Strategy

Cherian Samuel, Associate Fellow, Institute for Defence Studies and Analysis, India

Cherian Samuel

Cherian Samuel's presentation delved into how the perceived cyber-insecurity contributed to the development of India's national and international cybersecurity strategy. India has seen an unprecedented increase in Internet penetration. The number of broadband subscribers reached 55.2 million and overall Internet users are an estimated 200 million, making the country the third largest Internet user-base globally.

As India's population becomes more active in cyberspace, the risk of cyber-crime also increases. Cyber-crime rates registered under the India Information Technology Act have seen a dramatic rise from 420 in 2009 to almost 3000 in 2012. In India, the cybersecurity threat emanates from state actors as well as non-state actors. Referring to various international reports, Samuel maintained that there has been a persistent threat from state-sponsored actors in the form of trade espionage. The nature of cyber-attacks is also said to have shifted from passive attacks like spam to potential threats to critical infrastructure.

The emerging forms of cyber-insecurity led to a major reform of India's domestic and international cybersecurity strategy. Domestically, India has enacted a series of cybersecurity-related legislation, such as the 1998 IT Amendment Act to regulate data protection; the establishment of the Indian Computer Emergency Team (CERT-In) in 2004; and the IT Amendment Act 2008 that puts special emphasis on cyber-terrorism. India's cyber-policy was largely reactive and sporadic as evident in the fact that cyber-terrorism was only incorporated into the IT Amendment Act following the 2008 Mumbai Attack.

The National Cyber Security Policy (NSCP) was released in 2013 in an attempt to establish a comprehensive framework for India's cybersecurity strategy. NSCP is part of the three-part framework that includes the National Cyber Security Architecture and a National Cyber Security Strategy. It is aimed to create a secure cyberspace, strengthen the framework of India's cybersecurity strategy, promote public-private partnerships, and encourage research and development in cybersecurity. Additionally, India recently established a National Critical Infrastructure Protection Agency to respond to emerging threats to critical infrastructure.

At the international level, India has expressed strong support for and actively participated in international cyberspace CBMs through bilateral as well as multilateral frameworks. India has initiated bilateral cybersecurity dialogues with various countries including Japan, South Korea, the United Kingdom, and the US. India was also a member of the three United Nations Groups of Governmental Experts (UN GGE) on cybersecurity. Such active participation, Samuel argued, was driven by India's interest in the restructuring of global Internet governance to be more open, transparent and democratic.

India, however, has not been as active in regional cybersecurity cooperation. Regional cooperation for cybersecurity in Asia still lags behind largely due to mutual distrust, lack of institutional mechanisms, and differing capacities among Asian countries in dealing with cybersecurity issues. This was said to be the reason why India has wider cooperation with countries outside Asia than within.

Samuel concluded by re-emphasising the need for India to improve capacity building at home to create a more secure cyberspace as well as protect critical infrastructure, and improve bilateral and international cooperation in the areas of Internet governance and law enforcement cooperation in cybersecurity.

Discussion

One of the questions raised during the discussion

session was whether the mushrooming of regional and international fora for cybersecurity would create more problems than solutions. It was argued that theoretically speaking, seeing cybersecurity through regime theory was indeed problematic because regime theory regards legal regimes as an end to itself. But in reality, regimes can become outdated or in some cases, states may simply not abide by them, as the regime in question may limit their range of action. The counter argument is that the proliferation of international regimes is not necessarily problematic because the more efforts to create regimes, the more communication channels are available even in times of crisis. It was also mentioned that regime proliferation could indeed be justified for different problems need to be handled differently and by different institutional mechanisms.

The issue of applicability of the OSCE experience in cybersecurity cooperation to other regional frameworks including ASEAN was also discussed. It was noted that while the OSCE's experience was mixed, it could nevertheless provide valuable lessons in terms of the political processes of cooperation. However, it was also suggested that as each regional framework has different characteristics, the extent to which the OSCE experience could be applied to ASEAN is unclear. The progress of cybersecurity cooperation in the ASEAN Regional Forum (ARF) would depend in part on how the member states could pull together their technical and policy expertise to create effective measures.

Rapporteur: Navhat Nuraniyah

PANEL 4:

EFFORTS OF INTERNATIONAL ORGANISATIONS AND NGOS IN DEVELOPING CBMS

Developments in the Field of Information and Telecommunications in the Context of International Security: The UN Group of Governmental Experts

Zhang Jing, Office for Cyber Affairs, Chinese Ministry of Foreign Affairs, People's Republic of China

Zhang Jing

Zhang Jing spoke about China's contributions to international efforts in maintaining security and stability in cyberspace. She discussed at length the country's role in the Group of Governmental Experts (UN GGE). According to Zhang, the UN GGE is an important mechanism for international peace and security, committed to the in-depth and pragmatic study of cyber-issues, and shaping the future direction of cyberspace.

The first UN GGE was established in 1998 when Russia put forward a draft resolution for the use of Information and Communication Technologies (ICT) in the First Committee of the UN General Assembly entitled "Information and Communication Technology Developments in the Context of International Security." The resolution called for all parties to deal with the use of ICTs in the context of international peace and security. The UN's First Committee adopted the resolution of the same name every year, giving authority to all previous GGEs and those in the future. The discussion of previous meetings of the GGE focused on the evaluation of risks and recommendations on how to strengthen the collaboration for international norms to combat cyber-crimes as well as capacity building. After 10 years of evaluations, the mechanism reached a state of relative maturity, gaining wide acknowledgement from the international community. For the past decade, the discussions in the GGE have deepened along with the development in ICTs and the developments in the realm of cybersecurity.

The latest UN GGE report published in June 2013 noted remarkable progress in international efforts to promote a "peaceful, secure, open and cooperative cyberspace". It acknowledges the importance of applying norms derived from existing international law that are relevant to the use of ICTs by states. The report also suggests that additional norms could be developed in future. The principle of state sovereignty is affirmed in the report. While helping address the pressing concerns raised by the development of ICT technology, the UN GGE is interested in laying a foundation for cyberspace in the interest of all, through deliberation on the norms and rules bolstering the architecture of cyberspace.

Zhang observed that some people have argued that existing norms and laws are sufficient to address the challenges of cyberspace, and therefore, have refused to consider any new or additional norms. China, however, is of the opinion that the development of international law has not changed the order of cyberspace, and that the basic norms governing international relations are anchored in the UN Charter. Thus, behaviour in cyberspace should abide by the basic norms established, which include non-interference in the affairs of other countries, prohibition of the use of force, as well as peaceful resolution of disputes. However, given the unique attributes of cyberspace, the international community needs to find agreement on which of the existing rules can be applied to cyberspace; a question China believes should be posed to the international community. It is for this reason that China has repeatedly advocated for the enlargement of membership of the GGE. Zhang argued that there is the need to listen to the concerns of developing countries that are latecomers to ICT in order to take into account voices from different cultural and socio-economic backgrounds. The subsequent expansion of

membership in the GGE to 20 countries instead of the original 15 in 2014-2015 was regarded as a positive step by China.

Zhang concluded her presentation with an update of GGE activities. The next GGE will convene on 21-25 July 2014. It will focus on two areas: firstly, there will be continuing in-depth study of international norms and rules in international peace and security, which aims to lay the foundation for a code of conduct in cyberspace. Secondly, the GGE will study new issues pertaining to cyberspace such as privacy.

Cyber CBMs: A Multilateral Perspective

Ben Baseley-Walker, Programme Lead, Emerging Security Threats Programme, United Nations Institute for Disarmament Research

Ben Baseley-Walker

Ben Baseley-Walker discussed the international community's attempts to understand whether established national and international approaches to concepts such as sovereignty and law-making could be effectively applied to cyberspace. He also talked about how to address the new challenges raised by the borderless and dynamic nature of cyberspace itself. The borderless nature of cyberspace greatly impacts international relations and consequently, stability in the cyber-domain does reflect the existing ebbs and flows in international tensions. CBMs play a key role in developing the foundations for progress towards a stable and resilient cyber-regime. However, its organisation is still a subject of discussion and debate. While various regional organisations such as the OSCE, OAS and the ASEAN Regional Forum have made significant progress in discussing cyber-CBMs, defining the scope of CBMs and how they fit into multilateral norm development is a work in progress.

Baseley-Walker observed that there is a growing pervasiveness of cyberspace applications throughout government activities, industrial and civil processes and financial systems. Nearly all states, especially major global economic players, are heavily cyber-reliant. However, the international community is still struggling to understand if and how established national and international approaches to concepts such as sovereignty and law-making can be effectively applied to cyberspace as well as how to address the emerging challenges resulting from the borderless and dynamic nature of cyberspace.

In the context of cyber-stability, he highlighted that cyberspace is not a domain that can be insulated from international relations. Stability in the cyber-domain is reflective of the existing ebbs and flows in international tensions. Therefore inter-state instability must be prevented from spreading to the cyber-domain. Ideally, the absence of an established "code" of strategic messaging or a common understanding of escalation control in the cyber-domain should not lead to cyber-activities becoming a trigger for instability in traditional security domains. Whilst states may have very different political understandings of how to approach cyberspace, growing universal cyber-dependence on cyberspace necessitates that the goal of a stable and resilient cyber-regime can only be achieved collectively. CBMs play a key role in developing the foundations for progress towards this goal. Outside of the security calculus of major states' relations, the consolidation of norms of behaviour in cyberspace is very important.

The work of various regional organisations including the OSCE, the OAS and the ASEAN Regional Forum have made significant progress in discussing cyber-CBMs. Baseley-Walker argued that it is critical to look at the work of these organisations in defining the scope of CBMs and how they fit into the greater picture of multilateral norm development. From the perspective of UNIDIR, CBMs play a central role in mitigating vulnerabilities. He noted that building resilience in international relationships is the first step in working towards potentially binding multilateral agreements in the future. CBMs are crucial in translating

commonalities of interest and understanding of the cyber-domain. He stated that the international community should continue its discussion on defining acceptable behaviour in cyberspace. He concluded by suggesting that the work of the next round of the GGE must focus on the pragmatic and practical realities of cyber-governance.

The Role of Civil Society in Furthering CBMs

Daniel Stauffacher, President, ICT4 Peace Foundation

Daniel Stauffacher

Daniel Stauffacher observed that civil society participation in the development of national cybersecurity strategies or in regional and international CBMs processes has been minimal. This is surprising given that citizens, civil society organisations, as well as business and academia are core links in the ICT value chain, and the fact that their collective expertise is fundamental to resolving many of the core technical problems inherent in the ICT landscape. Civil society organisations have entered the discussion on security in cyberspace at a late stage; and seem focussed only on the impact the international security dimensions of ICTs will have on human rights, development and governance issues.

This phenomenon has been compounded by the uncertainty in the international environment, which has resulted from important geo-political shifts contributed to the sense of complexity and mistrust surrounding discussions and debates on cyberspace and the uses of ICTs for attaining political, military or economic advantage. This reality has undermined confidence and trust between states, as well as between states and their citizens.

Important breakthroughs for civil society participation in CBM were made in 2013. First, the UN GGE Report formally acknowledged the role of civil society in building cooperation for a peaceful, secure, resilient and open ICT environment. The report also recognised the role of civil society as well as that of the private sector in supporting government efforts in developing and implementing CBMs and exchanging information.

Stauffacher also discussed the possible roles of civil society and businesses in furthering cybersecurity-related CBMs, particularly in the areas of: (a) Transparency and Accountability; (b) Participation; and (c) Deepening the Knowledge Base.

In relation to transparency and accountability, the public domain, until very recently, held little information on international, regional and bi-lateral processes on cybersecurity. Many of these discussions therefore received little scrutiny from business and civil society. To address this, business and civil society organisations can develop tools to monitor their own government's role in international, regional and bi-lateral discussions on CBMs and norms. Knowledge regarding progress or setbacks in international and regional processes relating to CBMs and norms could also be made readily available to the public, and public discussions may be organised around them. Budgetary expenditure in the field of cybersecurity should be monitored to ensure an adequate balance between security, governance, development and human rights.

Staffaucher also noted that while security concerns have been raised with regard to making the processes relating to CBMs and norms too public, there is a push for more inclusivity. Business and civil society organisations can and therefore should lobby for their direct or indirect participation in developing CBMs, norms and other cybersecurity-related processes as suggested in the 2013 GGE report. Civil society groups can also further the development of CBMs by participating in capacity building efforts.

Staffaucher opined that deepening the knowledge base by enhancing knowledge and sharing information is central to building a secure and resilient ICT environment. It also helps to strengthen trust and confidence. Civil society can work more closely with the private sector and academia to ensure that evidence-

based research is made available to government representatives in discussions on developing CBMs and norms as well as to the broader public. Civil society and industry should develop stronger ties with academia and policy think-tanks to identify knowledge gaps and/or deepen the existing knowledge base. Furthermore, civil society can help trust-building efforts by bridging the understanding of regional and cultural differences.

Discussion

A participant inquired if NGOs could play a bigger role furthering CBMs at the bilateral and multilateral level. A speaker replied that NGOs may contribute through monitoring negotiations between states and publishing information on outcomes and processes to increase public awareness. Furthermore, they can provide assistance in preparing workshops, conferences, and debates to bring together representatives from different regions.

A participant inquired if an increase in UN GGE membership would enhance the process of the development of CBMs. A speaker replied that while the additional members would make reaching a consensus more challenging, it was envisaged that more voices would also result in the identification of more commonalities of interest as well.

A participant inquired as to how the development of CBMs could be further encouraged given competing national and regional interests. A speaker acknowledged that the development of national and regional-specific regulations could indeed result in norms that were not universally applicable. Moreover, CBMs were interpreted differently by various actors. Hence, efforts to increase global dialogue must be made so as to address these challenges.

Rapporteur: Jennifer Yang Hui

PANEL 5:

THE FUTURE OF INTERNET GOVERNANCE

What is Internet Governance and Where does it Currently Take Place?

Ang Peng Hwa, Professor and Director, Singapore Internet Research Centre, Nanyang Technological University

Ang Peng Hwa

Ang Peng Hwa began his presentation by explaining that the term governance refers not to government but the process of governing. That is, it embraces both rules as well as rules about the rules. There were currently two different approaches to Internet governance: One, where technical experts consult and make the rules, and two, where state representatives make decisions about the rules. To date, no consensus has been reached due in part to stakeholder interests.

Ang used the example of the Internet Corporation for Assigned Names and Numbers (ICANN)[1] controversy to illustrate the dynamics and complexities surrounding Internet governance. He pointed out that the Internet was in actuality governed by a 'dictator' in the form of ICANN. As questions were raised on whether ICANN would always behave benevolently and allow unfettered access to the Internet, attempts to develop an alternative governance regime at the international level were made.

The UN supported two-phase World Summit on the Information Society (WSIS) was initiated as a response. The first phase took place in Geneva in 2003[2], while the second phase[3] was held in Tunis in 2005. However, as discussions in the first phase did not lead to any agreements on how Internet governance would be carried out, the Working Group on Internet Governance (WGIG) was established to continue dialogue and come up with a plan of action for the second phase.

Among the major issues that emerged from the WGIG was: (a) the creation of the Internet Governance Forum (IGF)[4] to facilitate multi-stakeholder policy dialogue; (b) amendments to the existing oversight responsibilities of ICANN, which were designed to curtail US influence.

Another approach has been to seek amendments to the current International Telecommunications Regulations (ITRs). The UN's International Telecommunication Union (ITU) organised the World Conference on International Telecommunications (WCIT) in December 2012 for that purpose. However, this effort has been criticised by several entities including Google as being too state-centric, and possibly even information-restrictive. Some countries have also expressed their misgivings, and have refused to accept the amended ITRs. This means that there is still no consensus on Internet governance to date.

---

[1] The Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Internet Assigned Numbers Authority (IANA) functions, which are key technical services critical to the continued operations of the Internet's underlying address book, the Domain Name System (DNS). The IANA functions include: (1) the coordination of the assignment of technical protocol parameters including the management of the address and routing parameter area (ARPA) top-level domain; (2) the administration of certain responsibilities associated with Internet DNS root zone management such as generic (gTLD) and country code (ccTLD) Top-Level Domains; (3) the allocation of Internet numbering resources; and (4) other services. ICANN performs the IANA functions under a US Government contract (https://www.icann.org/resources/pages/welcome-2012-02-25-en). This effectively gives the US oversight of ICANN.

[2] The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake (https://www.itu.int/wsis/basic/about.html).

[3] The objective of the second phase was to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents (https://www.itu.int/wsis/basic/about.html).

[4] The Internet Governance Forum (IGF) is run by the IGF Secretariat. Its purpose is to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) with regard to convening a new forum for multi-stakeholder policy dialogue - the Internet Governance Forum (IGF) (http://www.intgovforum.org/cms/aboutigf).

Ang argued that a multi-stakeholder Internet approach involving not just governments but also industry and civil society was ultimately needed. He cited the Computer Security Incidence Response Team (CSIRT), Computer Emergency Response Team (CERT), work with NANGOG (North America Network Operators Group) and Council for Security Cooperation in the Asia Pacific (CSCAP) as possible incarnations of this approach.

Ang concluded by suggesting that Singapore needed to consider having a regional cooperation body for issues pertaining to Internet governance. He also cautioned that while it was essential to incorporate a variety of interests and perspectives into creating a global Internet governance framework, it was prudent to be aware of the existing tensions at the international level for doing so.

Singapore's Position on Internet Governance

John Yong, Director, Infocomm Security/Secure Systems Operations/Secure Communication, Infocomm Development Authority of Singapore

John Yong

John Yong's presentation was on Singapore's current position on Internet governance. He began by explaining the role of the Infocomm Development Authority of Singapore (IDA), which is a statutory board of the Ministry of Communications and Information (MCI). IDA's roles include: (a) telecoms sector regulator; (b) government's information technology and telecommunications office; and (c) national IT-Comms infrastructure developer. As Internet usage in both public and private sectors were increasing, it was necessary to pay attention to cybersecurity and Internet governance.

Internet governance covers a range of issues including: location of Internet resources (IP addresses and domain names); public policies; protection of intellectual property rights; international enforcement efforts against cyber-crime (e.g. hacking and spamming).

Yong explained that the Singapore government's approach to Internet governance is "pragmatic and non-ideological". It is based on four principles which guide IDA's actions.

First, IDA works to ensure that the Internet is accessible to all. This is envisaged to transform Singapore into a global, dynamic information and communications technology (ICT) hub and enable the country to leverage ICT for economic and social development. In operational terms, this is achieved through proactive reviewing of the regulatory framework to ensure there is healthy competition between Internet providers and ensuring that existing infrastructure is among the best across the globe. On this front, Yong stated that Singapore has invested heavily in the past decade to enhance its Internet connectivity with an extensive network of submarine cables. Yong also noted that IDA has initiated the National Broadband Network (NBN) with optical fibre cables to ensure high-speed access to the Internet at one gigabit per second.

Secondly, IDA promotes digital inclusiveness across all levels of Singapore society. IDA is involved with the 'New PC Plus' programme, which assists children from lower-income households to purchase new computers at subsidised prices and to provide access to broadband connection at no extra cost. IDA has also been involved in establishing programmes at local community centres to teach computer literacy through customised training for the physically challenged and/or elderly.

Thirdly, IDA focuses on securing the Internet space in Singapore through building and regularly updating their Infocomm security measures. Yong emphasised the importance of ensuring the population's ability to protect themselves from cyber-threats. He also emphasised that building a pool of cybersecurity professionals in Singapore is essential.

Finally, Yong noted that IDA believes in a multi-stakeholder approach to shape Internet governance where stakeholders in the private and public sectors can contribute meaningfully.

A Non-Profit Organisation's View on Internet Governance

Noelle de Guzman, Regional Programmes Coordinator for Asia Pacific, The Internet Society

Noelle de Guzman

Noelle de Guzman began her presentation with a brief introduction of The Internet Society and how it operated. She explained that the organisation works for the open development and evolution of the Internet. The organisation also believes that the decentralised and collaborative manner by which the Internet has been managed is key to its growth and importance as a global resource.

She then discussed the impact of current trends of Internet governance. The recent announcement by the US government that it will transition key Internet domain name functions to the global multi-stakeholder community could bring forth a more globalised and inclusive model of Internet governance. At the same time, the upcoming International Telecommunications Union (ITU) Plenipotentiary Conference, where the foundational ITU treaties will be reviewed and possibly revised, might also bring the global resource one step closer to possible fragmentation and state control.

Other intervening events in 2014 however, such as NET Mundial, hold great significance as they provide an opportunity for a variety of stakeholders to discuss Internet governance. The NET Mundial multi-stakeholder statement provided a roadmap and a set of principles for the future of Internet governance. These principles concentrated on several areas: (a) the need for a multi-stakeholder approach that is inclusive, transparent and accountable; (b) addressing the interests of those that are online as well as those who are yet to go online; (c) each stakeholder does not have defined roles and responsibilities, instead the respective roles and responsibilities of stakeholders must be interpreted according to the issue at hand; (d) facilitate more sustained coordination and information-sharing among existing forums and stakeholders, particularly between technical and non-technical communities; and (e) grounding Internet governance efforts in international human rights principles, including freedom of speech, freedom of association, and the right to privacy.

De Guzman also discussed the World Telecommunications Development Conference 2014. She noted that while the conference did not directly discuss Internet governance, the conference did produce the 'Dubai Action Plan'. This plan suggests that to promote widespread and affordable Internet access, there is a need for: (a) international cooperation, coordination and information-sharing on ICT access; (b) an enabling environment that is conducive to ICT development and the development of networks, applications and services; (c) promotion of digital inclusion with concentrated assistance to countries in need; and (d) enhancing confidence and security in ICT use.

De Guzman noted that the Internet Society is pursuing several principles, mirroring those of NET Mundial, including: (a) the multi-stakeholder model of Internet governance; (b) meaningful participation and inclusiveness to maintain a global and interoperable Internet; (c) the strengthening of existing Internet governance arrangements; (d) preserving the open architecture of the Internet; and (e) ensuring the Internet continues to be an interconnected and unfragmented space.

De Guzman concluded by stressing that there is not, and never will be, absolute security on the Internet – there will always be vulnerabilities. She added that security paradigms should be grounded on protecting the Internet as a global asset, rather than simply preventing perceived harm. De Guzman opined that the end goal of Internet security measures should be to make the Internet more resilient.

Discussion

A participant asked whether the idea of the classical Westphalian nation state is at odds with the idea of an inclusive approach to Internet governance. A speaker responded that while the concept of state sovereignty may overlap with an inclusive Internet governance approach, state structures are capable of evolving. The speaker also added that adopting a multi-stakeholder model in Internet governance does not demand that a state cedes all aspects of its sovereignty.

Another participant observed that most of the discussions on Internet governance provide top-down approaches to deal with cybersecurity. As such, the participant asked what could be done to achieve common cyber-norms at the ground level. A speaker replied that there were fundamental differences between cybersecurity and Internet governance. More importantly, Internet governance covers a range of areas, and cybersecurity was merely one of them. Another speaker noted that there are cyber-norms being developed with input provided by civil society groups, such as the Internet Society.

A participant asked whether the fact that the Working Group on Internet Governance (WGIG) recommended four different models, three of which gave primacy to governments, represented the dominant thinking about Internet governance. A speaker replied that government representatives in the WGIG undoubtedly influenced the four models that were recommended.

Rapporteur: Eliane Coates

PANEL 6:

HOW TO SECURE CYBERSPACE? THREE PRIVATE SECTOR PERSPECTIVES

Insuring Against Cyber Threats

Scotland Walsh-Riddle, Financial Lines Manager/Head of Directors and Officers, Southeast Asia, AIG Asia Pacific Insurance

Scotland Walsh-Riddle

Scotland Walsh-Riddle's presentation focussed on insurance against cyber-risks/threats. He observed that IT-related costs are mounting, and cyber-threats are now considered a top priority by many companies. A broader awareness of these issues is growing in Asia particularly since the number of threats is also growing. In 2009, only seven jurisdictions in the region had data privacy regimes and most of these were limited in scope. Now however, it is hard to find a jurisdiction without a data privacy regime and some have even been strengthened. However, data is not always located within one jurisdiction and modern businesses do not simply access the Internet, they operate entirely within it. Furthermore, the lines between personal use and business transactions are blurring.

In Walsh-Riddle's view, digital risks include: (a) Operational, which can arise from a lack of internal processes; (b) Financial risk that arises from fraud or theft; (c) Intellectual property (IP) risks where a loss of product or critical IP damages a company's ability to compete; (d) Legal and regulatory risks; and (e) Reputation risks that can cause harm to a business and its brand or reputation, since it can take years to build such reputation but one data breach can destroy it. With regard to cyber-risk, he argued that it should be handled in three key ways: (a) stronger public-private collaboration; (b) stronger and more sophisticated risk management; and (c) specialised insurance. International bodies cannot act alone, and as such, private sector participation is needed. Walsh-Riddle suggested that the best cybersecurity framework comprises people, processes and technology. All employees must be vigilant and have a security mentality, while senior management should prioritise cybersecurity within organisation-wide risk management. Processes need to be tested at least once a year and technology should be engrained in each company. Failing to train employees is significant since a company is only as strong as its weakest link, and employees tend to be the weakest link.

Walsh-Riddle then went on to discuss cyber-insurance coverage. First-party coverage is for direct losses incurred such as forensic investigations, business interruption losses, electronic data restoration, and cyber-extortion. Third-party coverage is for losses incurred by customers, for example credit card companies or for liabilities resulting from security breaches. Three aspects are covered under a policy: personal data, corporate data, and outsourcing. Walsh-Riddle further explained that the insurance market is evolving. For example, many companies conduct business completely on the cloud, and coverage now extends to cloud failure as it is considered network interruption.

To assess the premium, insurance companies usually consider the following issues: (a) What type of critical information does a client store and how is such information stored?; (b) What security controls are already in place and are they updated? (c) In which jurisdiction does the client operate?; (d) Does the company have a data protection policy in place?; (e) Does the company have a contingency plan, for example a back-up site?; and (f) To whom does the company outsource?

In conclusion, Walsh-Riddle explained that cyber-insurance is a relatively new product. In addition,

legislation is changing in Asia, and there are some growing pains in the market. He also observed that the data security market is not growing quickly enough, and that there is a need for more public awareness.

Networks on Fire: How to Defend Critical Government Networks

Bryce Boland, CTO, FireEye, Asia Pacific

Bryce Boland

Bryce Boland discussed defending critical government networks and the current state of cybersecurity globally in his presentation. He argued that there is a state of total compromise in most organisations today with security controls being bypassed on a constant basis. As a result, they are no longer effective in deterring attackers. He argued as there are no effective means for preventing malicious activity today, governments must take steps to protect themselves.

Boland explained that universities are often targeted in cyber-attacks for know-how as well as the fact that controls tend to be relatively lax compared to government organisations. He warned that contemporary malware is designed and created for use against a specific target. Approximately 75% of those attacks discovered by FireEye over the last six months were against a specific client. Traditional security applications like anti-virus software are no longer able to defend systems effectively. Boland observed that attackers generally do one of two things if a victim counters an attack: they either: (a) attack with a more sophisticated method; or (b) move downstream to smaller, less-protected targets. In the government domain, this means that attackers would most likely target government departments or smaller community organisations that have weaker protection rather than organisations that have strong protections like the military. And as information-sharing takes place between these departments, organisations that have strong protections could ultimately be compromised.

Boland observed that another area of concern is the lack of cybersecurity expertise. He argued that there is a real skills shortage that needs to be addressed. For instance, the number of cybersecurity professionals in Singapore dropped from 1,500 to 1,300 in one year, due in part to global demand. He suggested focusing on home grown talent and leveraging industry specialists to supplement skills. The provision of more training courses as well as opportunities for existing cybersecurity specialists to upgrade their skills would be helpful.

In conclusion, Boland argued that as security controls were currently blind to advanced attacks, they must be changed. Defences must not be static but dynamic such that they can both change and evolve constantly. Defences should comprise three elements: (a) People; (b) Processes; and (c) Technology. He also observed that governments are often challenged by bureaucratic procedures, and do not act fast enough. For instance, legislation can take years to enact, whereas malicious software are developed in weeks. Furthermore, the speed at which technology is acquired needs to change. Otherwise, security solutions run the risk of being outdated by the time they are implemented. The cost of security is also high because of the need for it to be maintained. Security should therefore be considered as a constantly evolving process and not as a one-time investment. Boland also recommended that a threat-centric mode of operation should be followed. This includes understanding the attacker and what it is they want to exploit, as opposed to what you are interested in protecting since there may be a difference.

Take Back Control with Cloud (Using Cloud for your Cyber Defence Strategy)

John Ellis, Enterprise Security Director, Akamai Technologies

John Ellis

John Ellis began by making three observations with regards to emerging cyber threats, and how to respond to them. First, the concept of a fixed perimeter was gone, that is, "de-perimeterisation" had become the new norm. Second, "the bad guys" were now global, sophisticated, automated, and highly distributed. Third, security strategy needed to go global, that is, control must be taken back with a globally distributed platform.

Ellis then discussed several issues that would have significant implications on the cyber landscape. First, 99% of malware targeted the android platform. Second, US$ 500,000 could be made on the open market for so-called zero-day malware for iOS. Third, although 47% of all Internet users were in Asia, the Internet penetration rate in Asia was low (est. 27.5%). Fourth, mobile was the biggest computing platform in developing countries. Lastly, by 2020 there would be approximately 4.7 billion people in Asia, which meant that while there was much space for growth and opportunities, there were also major challenges in light of the low Internet penetration rate.

Ellis argued that a key challenge was the inability of developing countries to protect themselves, especially in relation to cloud readiness, since the right legislation and infrastructure were currently not in place. He cited a recent report by the Australian Strategic Policy Institute (ASPI), which suggested that apart from Australia, Japan, Singapore and South Korea, many countries in the Asia-Pacific had not reached "Cyber Maturity" as yet. "Cyber Maturity" was a metric that assessed the "presence, effective implementation and operation of cyber-related structures, policies, legislation and organisations".[5]

Further commenting on cyber threats, Ellis pointed out that Asia made up 56% of the global attack traffic. For instance, most malicious traffic from botnets in 2013 originated from Indonesia, not China. He suggested that it was imperative to have a good functioning Internet even though 75% of web applications had some critical vulnerability. Distributed Denial of Service (DDoS) attacks were also a cause of concern, especially those involving hacktivists who attacked governments as well as cyber-criminals who employed DDoS as a distraction tactic to enable them to continue their criminal activities. For example, a denial of service attack against the White House was carried out last year whereby proxy attacks by state-sponsored hacktivist units (state-funded) targeted the US financial sector. Ellis expected that by 2016, attacks would be over 1 terabit per second and very difficult to withstand. He suggested that in light of these trends, there must be a transition away from the network centric approach to security since this was a game that could not be won by trying to plug every hole.

In conclusion, as traditional defences seemed to be inadequate and since 54% of malware was fully undetectable, Ellis argued that an "elastic network" approach to cybersecurity was needed, that is, the ability to use a globally distributed platform for defence. He also cautioned against turning off the Internet as a response, as this would severely constrain private businesses. Finally, he argued that data must be secured irrespective of where it resided, and encryption technology should be considered as a means to do so.

[5] The indicators include: whole-of-government policy and legislative structures, military organisation, business and digital economic strength and levels of social awareness of cyberspace.

Discussion

A participant asked whether cyber-insurance is different to other insurance policies given that it is dynamic, and whether customers with general insurance should purchase an additional cyber-insurance package. A speaker explained that it depends on what security controls are in place, and which industry is involved. In the US, assessors can be employed to evaluate an organisation's IT requirements and existing cybersecurity measures to determine what cyber-insurance products are relevant. There are several products available including data security liability, personal data liability, corporate data liability, outsourcing liability, defence costs and other comprehensive and/or tailored cyber-insurance policies. Coverage can also be provided under professional indemnity coverage or a fidelity policy that covers cyber-exposure. It is also possible to obtain a tailored cyber-insurance package.

A participant asked about strategies to counter cyber-criminal activities. A speaker replied that reducing the number of hiding spaces for cyber-criminals was a possible strategy. Also, ISPs could do more to detect compromised machines that are used to launch attacks. Another speaker suggested: (a) patching so that a system is up to date; (b) white-listing applications; and (c) matching systems to missions.

A participant asked how the Internet of Things (IoT)[6] could be better secured, to which a speaker replied that firewalls as a potential security measure are mere "bandaids" for the real problem of unsecure code that is written and never patched. It is fundamental, therefore, that the way in which computer technology is developed is changed to make it more robust from the beginning as opposed to building add-on security features later on.

Rapporteur: Caitriona Heinl

MODERATED DISCUSSION

Moderated Discussion
Wolff Heintschel von Heinegg, Professor, Public Law, Europa University Viadrina Frankfurt

Wolff Heintschel von Heinegg started the session by outlining the three main areas explored during the workshop: (a) Norms; (b) Confidence Building Measures (CBMs); and (c) Internet governance.

For norms, von Heinegg posed questions on the feasibility of actually achieving consensus among states. Interpretation of salient terms, especially for a dynamic subject area such as cyberspace, posed a great challenge. It was also highlighted that while global norms are the ideal standard, national rules and preferences would still take precedence for most countries. He also raised the question on the challenges faced in promoting human rights-based norms. Western European countries have more sophisticated appreciation of human rights relative to Asian countries; an asymmetry that could preclude the development of common policies.

Furthermore, von Heinegg highlighted that traditionally, it was states that dealt with human rights issues. In the context of cyberspace however, he pointed out that the private sector is a very important stakeholder. Finally, von Heinegg underscored the inherent tensions in reconciling the imperatives of security and individual freedoms in the use of cyberspace.

For CBMs, von Heinegg questioned whether a conclusion is even possible. He argued that in the setting of traditional efforts to further CBMs, states shared common threat perceptions. In cyberspace, however, threat perceptions are diverse, and as such, could pose an obstacle to the development of CBMs. Moreover, since technology changes rapidly, von

[6] The Internet of Things (IoT) is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (http://whatis.techtarget.com/definition/Internet-of-Things).

Heinegg claimed that agreements may be only useful for short periods of time.

Von Heinegg also talked about the difficulty of predicting future technological trends, critically assessing the utility of looking at past experiences such as negotiations for nuclear disarmament mechanisms. He also challenged the current pre-occupation for the procedural aspects of CBMs; whether they were sufficient to instil good behaviour.

On the issue of Internet governance, von Heinegg stressed how the theme of multi-stakeholder approaches was a recurring theme throughout the workshop. And while this apparent convergence of thought was welcomed, von Heinegg reminded the participants that such politically-correct and diplomatic sentiments do not easily translate into actual governance. The initial hurdle he argued is determining who the relevant stakeholders in cybersecurity are. Once the proper stakeholders are identified, the critical challenge of ensuring these actors' legitimacy, pose the next challenge. Von Heinegg cautioned that debates over Internet governance should be conscious of potential duplicity by "self-appointed guardians of self-appointed interests". Related to legitimacy issues is the degree in which states would relinquish control. Von Heinegg expressed the need for tempered expectations, citing an apparent "renaissance of sovereignty" among state actors.

In conclusion, von Heinegg noted that: First, cybersecurity remains a conceptually broad term that needs to be rethought. Putting everything in one "basket" could make finding answers more difficult. Hence, von Heinegg recommended considering more narrow conceptions of cybersecurity. Second, the reliance of societies and individuals to cyberspace was juxtaposed to the limited consideration of national security imperatives. Neglect of security interests, he argued, is the root of piecemeal efforts by states to "regain" cyberspace.

Discussion

A participant asked if it was possible to reconcile the intent to establish CBMs in the light of increased initiatives to legitimise widespread use of the law of countermeasures. The collective response from the audience was that force should be the last resort when responding to attacks launched through and from cyberspace.

The discussion then shifted to the diversity of threats under the umbrella of cybersecurity, and consequently the emergence of diverse interests. It was pointed out that cybersecurity issues are akin to prior and ongoing debates in terrorism studies. For both issues there is still no "big tent" that could delineate the policy challenges. Stakeholders would be better off crafting more practical definitions of cybersecurity of "smaller tents" to facilitate cooperation. While appearing pedantic, definitions based on common denominators could lead to huge impacts in the future.

Rapporteur: Joseph Franco

WORKSHOP AGENDA

Thursday, 3 July 2014
Cybersecurity CBMs and Norms

0830 – 0930hrs **Registration**
Venue : Pacific Ballroom Foyer (Level 1)

0930 – 0945hrs **RSIS Corporate Video + Welcome Remarks**
by **Kumar Ramakrishna**, *Head, Centre of Excellence for National Security (CENS), RSIS*
Venue : Pacific 3 (Level 1)
Attire : Smart Casual (Long-Sleeved shirt without tie)

0945 – 1045hrs **Keynote Address: Cybersecurity 2014: Key Trends and Issues**
Venue : Pacific 3 (Level 1)

Chairperson :
Kumar Ramakrishna, *Head, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
Irving Lachow, *Principal Cyber Security Engineer, The MITRE Corporation*

Q & A

1045 – 1100hrs **Tea Break**
Venue : Pacific Ballroom Foyer (Level 1)

1100 – 1230hrs **Panel 1: Cybersecurity and Cyber-Insecurity: How Serious is the Threat?**
Venue : Pacific 3 (Level 1)

Chairperson :
Kumar Ramakrishna, *Head, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
A (Technical) Introduction to Cyber-Insecurity for Policymakers *by* **David Senty**, *Director, Cyber Operations, The MITRE Corporation*

Strategic Threats and The Way Out *by* **Kah Kin Ho**, *Head of Strategic Security, Corporate Technology Group, Cisco Systems*

The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth *by* **Erik Gartzke**, *Professor, Dept. of Political Science, University of California, San Diego and Professor of Government, University of Essex*

Q & A

1230 – 1345hrs **Lunch**
Venue : Pacific 2 (Level 1)

1345 – 1545hrs **Panel 2: Emerging Norms for Cyberspace**
Venue : Pacific 3 (Level 1)

Chairperson :
Caitríona H. Heinl, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
The Tallinn Manual: The Laws of Cyberwar *by* **Wolff Heintschel von Heinegg**, *Professor, Public International Law, European University Viadrina*

How do Human Rights Apply to Cyberspace? *by* **Joy Liddicoat**, *Human Rights Specialist, Association for Progressive Communications*

Regulatory Best Practices to Fight Cybercrime *by* **Cormac Callanan**, *Owner/Founder, Aconite Internet Solutions*

Active Cyber Defence *by* **Irving Lachow**, *Principal Cyber Security Engineer, The MITRE Corporation*

Q & A

1545 – 1600hrs **Tea Break**
Venue : Pacific Ballroom Foyer (Level 1)

1600 – 1730hrs **Panel 3: What Role can Confidence Building Measures play to Enhance Cybersecurity?**
Venue : Pacific 3 (Level 1)

Chairperson :
Norman Vasu, *Deputy Head, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
[SKYPE] US-Russian Confidence Building Measures for Cyberspace *by* **Oleg Demidov**, *Program Director, The Russian Center for Policy Studies*

Applying Insights gained from Traditional CBMs to Cyberspace *by* **Ulrich Kuehn**, *Researcher, Institute for Peace Research and Security Policy, University of Hamburg*

India's International Cybersecurity Strategy *by* **Cherian Samuel**, *Associate Fellow, Institute for Defence Studies and Analysis*

Q & A

1730hrs **End of Day 1**

1830 – 2100hrs **Workshop Dinner (by invitation only)**
Venue : Edge, Pan Pacific Singapore (Level 3)

Friday, 4 July 2014
CBMs, Internet Governance, and Private Sector Contributions to Cybersecurity

0830 – 0930hrs **Registration**
Venue : Pacific Ballroom Foyer (Level 1)

0930 – 1100hrs **Panel 4: Efforts of International Organisations and NGOs in Developing CBMs**
Venue : Pacific 3 (Level 1)

Chairperson :
Sulastri Osman, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
Developments in the Field of Information and Telecommunications in the Context of International Security: The UN Group of Governmental Experts *by* **Zhang Jing**, *Officer for Cyber Affairs, Chinese Ministry of Foreign Affairs, People's Republic of China*

Cyber CBMs: A Multilateral Perspective *by* **Ben Baseley-Walker**, *Programme Lead, Emerging Security Threats Programme, United Nations Institute for Disarmament Research (UNIDIR)*

The Role of Civil Society in Furthering CBMs *by* **Daniel Stauffacher**, *President, ICT4 Peace Foundation*

Q & A

1100 – 1115hrs **Tea Break**
Venue : Pacific Ballroom Foyer (Level 1)

1115 – 1245hrs **Panel 5: The Future of Internet Governance**
Venue : Pacific 3 (Level 1)

Chairperson :
Damien D. Cheong, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
What is Internet Governance and where does it currently take place? *by* **Ang Peng Hwa**, *Professor and Director, Singapore Internet Research Centre, Nanyang Technological University*

Singapore's Current Position on Internet Governance *by* **John Yong,** *Director, Infocomm Security/Secure Systems Operations/Secure Communication, Infocomm Development Authority of Singapore*

A Non-Profit Organisation's View on Internet Governance *by* **Noelle de Guzman**, *Regional Programmes Coordinator for Asia Pacific, The Internet Society*

Q & A

1245 – 1400hrs **Lunch**
Venue : Pacific 2 (Level 1)

1400 – 1530hrs **Panel 6: How to Secure Cyberspace? Three Private Sector Perspectives**
Venue : Pacific 3 (Level 1)

Chairperson :
Bilveer Singh, *Adjunct Senior Fellow, Centre of Excellence for National Security (CENS), RSIS*

Speakers :
Insuring Against Cyberthreats *by* **Scotland Walsh-Riddle**, *Financial Lines Manager/Head of Directors and Officers – Southeast Asia, AIG Asia Pacific Insurance*

Networks on Fire: How to Defend Critical Government Networks *by* **Bryce Boland**, *CTO, FireEye, Asia Pacific*

Take Back Control with Cloud (Using Cloud for your Cyber Defence Strategy) *by* **John Ellis**, *Enterprise Security Director, Akamai Technologies*

Q & A

1530 – 1545hrs **Tea Break**
Venue : Pacific Ballroom Foyer (Level 1)

1545 – 1630hrs **Moderated Discussion on Key Takeaways**
Venue : Pacific 3 (Level 1)

Chairperson :
Wolff Heintschel von Heinegg, *Professor, Public International Law, European University Viadrina*

1630hrs **End of Day 2**

1830 - 2030hrs **Closing Dinner (by Invitation Only)**
Venue : Hai Tien Lo, Pan Pacific Singapore (Level 3)

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

Ang Peng Hwa
Professor and Director
Wee Kim Wee School of Communication and Information
Nanyang Technological University
76 Nanyang Drive
Basement 4, Block N2.1
N2.1-B4-01
Singapore 637331

Ben Baseley-Walker
Programme Lead
Emerging Security Threats Programme
United Nations Institute for Disarmament Research (UNIDIR)
Palais des Nations
CH 1205 Geneva
Switzerland

Bryce Boland
Vice President/CTO
Asia Pacific
FireEye, INC.
Unit 1, 38th Floor
AXA Tower
8 Shenton Way
Singapore 068811

Cormac Callanan
Owner/Founder
Aconite Internet Solutions
424 Richmond Court
Richmond Avenue South
Dublin 6
Ireland

Oleg Demidov
Program Director
International Information Security and Global Internet Governance
The Russian Center for Policy Studies
P.O. Box 147
Moscow, 119019, Russia

John Ellis
Director, Enterprise Security
Asia Pacific & Japan (APJ)
Akamai Technologies, Inc.
1 Raffles Place
16-61 One Raffles Place Tower 2
Singapore 048616

Erik Gartzke
Associate Professor
Department of Political Science
University of California, San Diego
9500 Gilman Drive/Office: 327 SSB
Department of Political Science, 0521
La Jolla, CA 92093-0521
USA

Noelle de Guzman
Regional Programmes Coordinator, Asia-Pacific
Internet Society
9 Temasek Boulevard
#09-01 Suntec Tower Two
Singapore 038989

Wolff Heintschel von Heinegg
Professor, Public International Law
European University Viadrina
Postfach 1786
15207 Frankfurt (Oder)
Germany

Kah Kin Ho
Head, Strategic Security
Cisco Systems
Avenue des Uttins 5
1180 Rolle
Switzerland

Ulrich Kuehn
Researcher
Institute for Peace Research and Security Policy
University of Hamburg
Beim Schlump 82
20144 Hamburg
Germany

Irving Lachow
Principal Cyber Security Engineer
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22101
USA

Joy Liddicoat
Human Rights Specialist
Association for Progressive Communications
PO Box 29755
Melville 2109
South Africa

Cherian Samuel
Associate Fellow
Institute for Defence Studies and Analysis
1 Development Enclave
Rao Tularam Marg
New Delhi 110 010
India

David Senty
Director, Cyber Operations
The MITRE Corporation
7594 Colshire Drive
M/S N610
McLean, VA 22102
USA

Daniel Stauffacher
President
ICT4 Peace Foundation
Place Saint-Gervais 1
Case postale 5349 1211
Genève 11
Switzerland

Scotland Walsh-Riddle
Financial Lines Manager/Head of Directors and Officers
Southeast Asia
AIG Asia Pacific Insurance Pte. Ltd.
AIG Building
78 Shenton Way #07-16
Singapore 079120

John Yong
Director, Infocomm Security & Assurance Division
Infocomm Development Authority of Singapore (IDA)
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438

Zhang Jing
Officer for Cyber Affairs
Chinese Ministry of Foreign Affairs
No. 2 Chaoyangmen Nandajie
Chaoyang District
Beijing 100701
People's Republic of China

CHAIRPERSONS

Damien D. Cheong
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

Caitríona H. Heinl
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

Sulastri Osman
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

Bilveer Singh
Adjunct Senior Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

Norman Vasu
Senior Fellow and Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue
Singapore 639798

ABOUT CENS

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

Why CENS?

In August 2004 the Strategic Framework for National Security outlined the key structures, security measures and capability development programmes that would help Singapore deal with transnational terrorism in the near and long term.

However, strategising national security policies requires greater research and understanding of the evolving security landscape. This is why CENS was established to increase the intellectual capital invested in strategising national security. To this end, CENS works closely with not just other RSIS research programmes, but also national security agencies such as the National Security Coordination Secretariat within the Prime Minister's Office.

What research does CENS do?

CENS aspires to be an international research leader in the multi-disciplinary study of the concept of resilience in all its aspects, and in the policy-relevant application of such research in order to promote security within and beyond Singapore.

To this end, CENS conducts research in three main domains:

- *Radicalisation Studies*
  The multi-disciplinary study of the indicators and causes of violent radicalisation, the promotion of community immunity to extremist ideas and best practices in individual rehabilitation.

- *Social Resilience*
  The inter-disciplinary study of the various constitutive elements of social resilience such as multiculturalism, citizenship, immigration and class. The core focus of this programme is understanding how globalized, multicultural societies can withstand and overcome security crises such as diseases and terrorist strikes.

- *Homeland Defence*
  A broad domain researching key nodes of the national security ecosystem. Areas of particular interest include the study of strategic and crisis communication, cyber security and public attitudes to national security issues.

How does CENS help influence National Security Policy?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organises courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

How does CENS help raise public awareness of National Security issues?

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence-related publications, as well as write op-ed analyses in leading newspapers. Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as radicalisation and counter-terrorism, multiculturalism and social resilience, as well as crisis and strategic communication.

How does CENS keep abreast of cutting edge National Security research?

The lean organisational structure of CENS permits a constant and regular influx of Visiting Fellows of international calibre through the Distinguished CENS Visitors Programme. This enables CENS to keep abreast of cutting edge global trends in national security research.

For more information about CENS, visit http://www.rsis.edu.sg/cens

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** was established in January 2007 as an autonomous School within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education with a strong practical emphasis,
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy,
- Foster a global network of like-minded professional schools.

Graduate Education in International Affairs

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (MSc) degree programmes in Strategic Studies, International Relations, Asian Studies, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from more than 50 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS.

A small but select PhD programme caters to advanced students who are supervised by faculty members with matching interests.

Research

Research takes place within RSIS' six components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National

Security (CENS, 2006), the Centre for Non-Traditional Security Studies (Centre for NTS Studies, 2008); the Temasek Foundation Centre for Trade & Negotiations (TFCTN, 2008); and the Centre for Multilateralism Studies (CMS, 2011). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

The school has five professorships that bring distinguished scholars and practitioners to teach and to conduct research at the school. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, the NTUC Professorship in International Economic Relations, the Bakrie Professorship in Southeast Asia Policy, and the Peter Lim Professorship in Peace Studies.

International Collaboration

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABOUT NSCS

The **National Security Coordination Secretariat (NSCS)** was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is Deputy Prime Minister and Minister for Home Affairs Mr Teo Chee Hean.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr Benny Lim, who is concurrently Permanent Secretary (National Development) and Permanent Secretary (Prime Minister's Office).

NSCS comprises two centres: the National Security Coordination Centre (NSCC) and the National Security Research Centre (NSRC). Each centre is headed by a Senior Director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipation of strategic threats. It also organises and manages national security programmes, one example being the Asia-Pacific Programme for Senior National Security Officers, and funds experimental, research or start-up projects that contribute to our national security.

For more information about NSCS, visit http://app.nscs.gov.sg/public/home.aspx

RSiS Nanyang Technological University | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University

Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798

Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg