CYBERSECURITY: EMERGING ISSUES, TRENDS, TECHNOLOGIES & THREATS IN 2015 AND BEYOND

Event Report
20-21 July 2015

Centre of Excellence
for National Security

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

Event Report

CYBERSECURITY: EMERGING ISSUES, TRENDS, TECHNOLOGIES & THREATS IN 2015 AND BEYOND

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:
Nur Diyanah Binte Anwar, Priscilla Cabuyao, Joseph Franco, Dymples Leong Suying, Romain Brian Quivooij, Tan E Guang Eugene, Jennifer Yang Hui and Yeap Su Yin

Editor:
Caitríona H. Heinl

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

Welcome Remarks

Shashi Jayakumar emphasised the timely nature of the workshop's theme, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond". He opined that technology is dynamic and constantly changing with newer threats and challenges consequently emerging. He highlighted that the general societal psyche and government policies on cybercrime have not kept up with developments in the cybersecurity domain. Jayakumar then highlighted CENS' role in bridging this gap through the workshop, as a think tank with applied focus through a higher degree of critical thinking. In this regard, he emphasised the important role that the CENS' Homeland Defence Programme continues to play in identifying gaps in cybersecurity discussions. Jayakumar thanked the speakers and participants for agreeing to participate and share their expertise, and encouraged discussions to continue beyond the workshop.

Opening Address

Ambassador Ong Keng Yong cited three recent developments where Singapore has been addressing cybersecurity issues. First, the benefits that Singapore's five-year National Cybersecurity Masterplan could bring in strengthening national resilience against cyber threats and protecting the country's critical infrastructure. Second, the formal launch of the Cyber Security Agency in overseeing the holistic development of Singapore's cybersecurity domains. Third, the opening of the INTERPOL Global Complex for Innovation, set to be an international leader in the fight against cyber-related crime, and in further defining cybercrime in international legislation. However, Ong acknowledged that these institutional structures are insufficient in today's rapidly changing technology-dependent environment. Therefore, he encouraged the speakers and participants to maximise their participation in the workshop by engaging in deeper discussions amongst academics and practitioners, and learning various best practices from an international network of specialists.

Keynote Address 1
Cyber Foreign Policy: Threats and Opportunities

Christopher Painter began his address by stressing how the U.S. State Department is increasingly looking at cyber matters from a policy perspective and not just as a technical issue. For instance, each U.S. diplomatic mission now has "cyber representatives". Painter then laid out Washington's view of cyber issues in East Asia and the Pacific. China, he observed, appeared more aggressive in promoting its government-centric vision of cyberspace, which emphasises "sovereignty over technology and information". Another issue of concern to the United States is the increasing use of illicit cyber tools for corporate espionage and commercial gain. Nonetheless, Painter remarked that there is optimism among American policymakers. He outlined the existence of cooperative initiatives that Washington is pursuing with Asia Pacific states such as Australia, Japan, South Korea, and Singapore. Transparency, he pointed out, is the key in stabilising the international community, in the face of expanding state-level offensive cyber capabilities. Painter concluded that any overarching framework for international security should allow for a shared response to common threats.

Panel 1
Cyber and International Security: Opportunities and Challenges for Further Cooperation

The first panel focused on the opportunities and challenges in fostering cooperation in cyber and international security. The first speaker, Wouter Jurgens, expanded on how cyberspace is a matter of strategic importance - this is an international issue affecting everyone; all stakeholders should be involved in negotiations; and more attention should be paid to cyber matters. The second speaker, Yono Reksoprodjo, observed that ASEAN is an entity based on confidence building measures, and the norms within the ASEAN community are respected. Reksoprodjo stressed the need to avoid the creation of a security paradox in cyberspace, and the importance of finding international and regional solutions for cyber in relation to issues like terrorism and separatism. The third speaker, Tobias

Feakin, noted that states are under huge pressure to react to cyber incidents, but warned that experiences in dealing with cyber incidents have been ad hoc in nature. Feakin noted that some level of preparation by states was necessary to determine the appropriate level of response to an incident.

Panel 2
Squaring National Security and Data Privacy Matters

Simon Chesterman's presentation considered the inherent tension between rights of citizens and the security concerns of governments. He argued that the purported trade-off fails to capture the complexity surrounding cyber issues. Chesterman opined that future limits to state power would likely come from private corporations that handle citizens' data, rather than legislation or government. Geronimo Sy began his presentation by presenting a legal framework that highlighted the nuances between cybersecurity and cybercrime in the Philippines. Sy stressed how cybercrime falls within the bounds of criminal law, and is not a completely novel challenge. He subsequently listed recent legislative initiatives, which include proposals to create 20 to 30 specialised "e-courts" to hear cyber-related cases. Bryan Tan presented Singapore's experience and perspective on cyber issues, shaped by the realisation that national security is no longer limited to the physical realm. Singapore's critical information infrastructure has nonetheless continued to adapt against evolving threats and plays an indispensable role in driving progress in the city-state. He argued that creativity is as important as safety.

Panel 3
Digital Economy

During this panel, Jan Neutze examined how public-private partnerships are essential to cybersecurity and provided insights on key trends amid an evolving landscape. Information sharing between the public and private sectors could ensure the development of overarching strategy for information sharing on actionable threats; clear government policies for handling vulnerabilities; as well as encourage the global sharing of best practices. Michael Mylrea elaborated that "smart cities" bring technology, government, and society together to enable: (a) a smart economy; (b) a smart environment; (c) smart living; (d) smart mobility; and (e) smart people. Smart cities are facing new threats such as the digitisation of critical infrastructure that could expose vulnerabilities, with software glitches that could result in massive amounts of data being open to hacking. Daniel Castro discussed the correlations between the economy and cybersecurity. He provided four observations: (a) recognise the economic consequences; (b) the need to reorient government strategies in cybersecurity; (c) develop new ways to restore trust between countries; and (d) the trend of populism in shaping technological policy debates.

Keynote Address 2
Cybersecurity Trends and Issues from a Singapore Perspective

John Yong explored the trends and opportunities associated with the building of a smart nation in Singapore. He explained the reasons for this development, including a dense, aging and technology-driven population. The success of this revolution relied on the commoditisation of hardware and the translation of big data into applications that citizens will find useful. Focusing his remarks on the centrality of digitisation, John Yong explained that ensuring a higher quality of life is a key objective. However, this is impossible to achieve without the implementation of an effective security system. Cyber vulnerabilities and malicious activities, such as defacement and hijacking of critical infrastructure, are examples of the sophisticated and evolving cybersecurity threat landscape. As a response, John Yong emphasised the importance of a multi-pronged counter-strategy. He concluded by presenting some of the key initiatives taken by Singapore in this domain, while stressing the need for a pervasive and adaptive cybersecurity architecture.

Panel 4
Cyber in Practice – Key Developments

Christophe Durand focused on the theme of convergence. He discussed efforts undertaken by INTERPOL to bridge approaches in combating cybercrimes and ensuring cybersecurity. While law

enforcement agencies are concerned with detecting, attributing and disrupting cybercrime networks, the private sector places importance on implementing protective and business continuity measures. Finding means to harmonise these approaches represents an important step in tackling cybercrimes. The next speaker, Wolfgang Roehrig, provided an in-depth analysis of the strategic approaches adopted by the European Union in developing cyber defence capabilities. Providing an overview of the implementation of the EU Cyber Defence Policy Framework, Roehrig cited a number of areas where improvements in cooperation are needed, including the need to enhance the integration of cyber defence capabilities in strategic areas. With regard to the theme of cooperation, the third speaker, Eugene Teo, highlighted the role of public-private partnerships in managing cyber attacks. The creation of a more dynamic information-sharing environment, where time-sensitive information is disseminated quickly to relevant parties across the public and private sectors, is a way to enhance this effort.

Discussion
The Global Implications of the U.S. - China Cyber Relationship

Zhu Qichao outlined the historical context and major challenges in China-U.S. cybersecurity cooperation. With the rapid development of China's national power and the corresponding expansion of its national interests in cyberspace, cybersecurity has become an important issue with great implications for the U.S.-China relationship. Zhu observed that there is currently limited communication and cooperation on cyber-related issues that would help ease tensions and facilitate strategic mutual trust between the two powers. Jason Healey's presentation outlined the U.S. position on international cybersecurity, including the similarities and differences with China's position. He then discussed international cyber norms, the application of international law to state behaviour in cyberspace, and the development of confidence building measures. Specific flashpoints in the U.S.-China relationship relating to cyber were also discussed. Finally, the dialogue highlighted the global impact of the U.S.-China cyber relationship.

Panel 5
Emerging Technology Trends and Threats

This panel focused on the legal implications of cyber warfare, India's cybersecurity landscape and the principles of deterrence and arms control in cyberspace. William Boothby discussed the nexus between the cyber domain and lethal autonomous systems. He explored the key notions of automation and autonomy as well as legal principles associated with cyber warfare. Rahul Sharma provided a description of the Indian cybersecurity ecosystem. He underlined the challenges associated with three major strategic issues: (a) national security; (b) Internet governance; and (c) privacy. Sean Kanuck provided conceptual clarifications on the notion of the cyber environment and frameworks for deterrence, disarmament, and arms control. Mapping the context of limitations on cyber activities, he offered his interpretation of cybersecurity architecture, which he based on the four principles of transparency, universality, enforceability and stability.

Closing Address
Technology, Threats and Trust in an Interconnected World

In the closing address, Robert Butler discussed several noteworthy themes highlighted during the workshop. In particular, he focused on the potential of technology, threats and trust to enable cybersecurity stakeholders to create a future with a strong foundation. For technology, he explained that the Internet of Things has demonstrated how far humans have come, as well as foreshadows where they are heading in terms of the ability to communicate. Regarding threats, the security vulnerability of devices, threat actors, and the importance of resilient structures in facing risks and danger, are significant. In terms of trust, he stressed the need for collaboration and partnerships in building a framework composed of elements that all stakeholders can espouse and achieve together.

Moderated Discussion on Key Takeaways

Sean Kanuck underlined the relevance of conferences and dialogues on cybersecurity (like the CENS workshop), in addressing current system

developments, potential risks and inevitable threats as well as challenges. For instance, Kanuck noted the rise of high-level policy attention for cyber foreign relations, the cyber international security dilemma, confidence building measures, and lessons learned from prominent cybersecurity incidents. Drawing from the presentations on data privacy, he asked important questions on the critical relationship between citizens, the government, freedom of speech, and sovereignty. Kanuck then discussed the importance of transparency, intelligence analysis and international cooperation, not only between governments, but also with private corporations. He pointed out that the workshop discussion on the U.S.-China cyber relationship is a confidence building measure in itself as it helps identify collective norms. He also argued that threats related to the Internet of Things and Smart Nation are expected to have major implications in the future.

WELCOME REMARKS

Welcome Remarks
Shashi Jayakumar, Head, Centre of Excellence for National Security (CENS), RSIS

Shashi Jayakumar

Shashi Jayakumar, in his welcoming remarks, explained that research on cybersecurity issues under the CENS Homeland Defence programme has been well received. This is one of the reasons why a workshop on cybersecurity is organised by CENS annually.

Referring to this year's theme, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Jayakumar suggested that while technology is constantly changing and dynamic, it is always accompanied by newer threats and challenges. He highlighted that the general societal psyche and government policies on cybercrime have not kept up with developments in the cybersecurity domain. In this regard, he highlighted CENS' role - as a think tank with applied focus through a higher degree of critical thinking - in bridging this gap. The CENS Homeland Defence programme continues to play an important role in identifying loopholes which should be bridged, identifying and researching areas susceptible to cybersecurity issues such as the aviation industry, and highlighting policy improvements which should be considered.

Jayakumar then outlined what the different panels covered over the two days. Panel One covered issues relating to cyber and international security - opportunities and challenges for further cooperation. Panel Two's theme was "Squaring National Security and Data Privacy Matters". Panel Three covered issues pertaining to the digital economy, Panel Four focused on "Cyber in Practice – Key Developments", while Panel Five covered emerging technology trends and threats. There were also discussions on the global implications of the U.S.-China cyber relationship and a keynote address on "Cyber Foreign Policy: Threats and Opportunities".

These sessions aimed to provide an international focus without ignoring the various cybersecurity concerns that Singapore faces. They highlighted several measures in deterrence, redlines in cybersecurity, norms and law enforcement. Additionally, the panels outlined the interplay between the public and private sector in securing the cyber domain – specifically in addressing how cybercrimes can affect critical infrastructure.

Jayakumar alluded that the speakers would bring timely discussions to the workshop, considering that they would be referring to several recent cyber attacks and case studies as pertinent examples. The expertise of the speakers and participants would also encourage high-level networking as well as encourage discussions from both a policy and theoretical perspective. Deeper and more robust discussions about topics covered in the panels would also be encouraged through the syndicate discussions, compared to the traditional question and answer session. Jayakumar encouraged everyone to network and learn from each other.

Contributed by Nur Diyanah Binte Anwar

OPENING ADDRESS

Opening Address

Ambassador Ong Keng Yong, Executive Deputy Chairman, RSIS

Ambassador Ong Keng Yong

Ambassador Ong Keng Yong introduced three recent developments in the way in which Singapore is addressing cybersecurity issues that are relevant to local and global concerns.

First, Ong referred to Singapore's five-year National Cybersecurity Masterplan and noted its benefits in strengthening national resilience against cyber threats and protecting Singapore's critical infrastructure. It will work towards improving the security and resilience of critical infocomm infrastructure and services, encouraging infocomm security adoption among businesses and Internet users, and increasing the number of Singapore's infocomm security experts.

Second, he spoke of the formal launch of the Cyber Security Agency of Singapore (CSA). The CSA maintains a central purview over Singapore's national cybersecurity functions and works with partners to engage in the holistic development of Singapore's cybersecurity domain. Third, he highlighted the opening of the INTERPOL Global Complex for Innovation (IGCI). He stated that the IGCI's primary purpose is to be an international leader in the fight against cybercrime and cyber-related crime.

However, Ong added that institutional structures such as the National Cybersecurity Masterplan, the CSA and the IGCI are insufficient in today's rapidly changing technology-dependent environment. He encouraged more workshops and forums that bring together expertise in the cybersecurity domain – such as the annual CENS Cybersecurity Workshop. Such platforms would allow for deeper discussions and exchanges among academics and practitioners, as well as allow for the exchange of best practices through an international network of specialists.

Ong suggested three areas that the speakers and participants could consider throughout the duration of the workshop. First, he encouraged deeper thinking on how policy-makers can protect cyberspace at the national level during a cyber attack or emergency, beyond what has already been done. He suggested that these further measures can also protect citizens and Internet users, while enabling the necessary information to be disseminated should a cyber attack occur.

Second, Ong challenged the speakers and participants to think of how governments can carry out policy work without disrupting or intruding into the functioning of various cyber domains. Third, Ong asked that they share some policy practices which are sensitive to the diversity of cultures present in their own societies, which may then be adapted locally in the Singapore context. He urged the speakers and participants to both contribute actively in discussions as well as maintain contacts.

Contributed by Nur Diyanah Binte Anwar

KEYNOTE ADDRESS

Keynote Address - Cyber Foreign Policy: Threats and Opportunities

Christopher M.E. Painter, Coordinator for Cyber Issues, Office of The Secretary, U.S. Department of State

Christopher M.E. Painter

Christopher Painter began his presentation by highlighting the greater salience of cyber issues in the U.S. State Department. At present, cyber issues are increasingly seen from the policy and not just technical perspective. American diplomatic missions now have dedicated "cyber representatives" tasked to look into cyber-related initiatives. Nonetheless, Painter admitted that cybersecurity and cyber policy as a whole remains nascent. Policy silos still remain among traditional cybersecurity stakeholders and other policy actors in government - such as foreign policy or human rights experts.

In terms of cyber foreign policy, both technical and policy threats are viewed as hurdles to cybersecurity. Technical threats fall into two categories: state and non-state attacks. Painter recalled the Sony Pictures and GitHub intrusions as examples of the widespread damage that could be wrought by state-sponsored cyber attacks. For non-state attacks, there is less emphasis on damage but on the level of disruption and the illicit financial gain that perpetrators can reap. In terms of policy threats, Painter highlighted how some governments are asserting their sovereignty on content production. Some countries are trying to replace the system of Internet governance - a multi-stakeholder system that involves governments, the private sector, civil society and academia. What is touted as a replacement is a state-only, multilateral system that would have technical, human rights and security implications that are not helpful to the global community. Some authoritarian governments are also trying to stymie the free flow of information to their populace, citing its destabilising tendency.

Painter then discussed Washington's perspective on East Asia and the Pacific. China is increasingly assertive and is pushing its government-centric vision of cyberspace. For Beijing, sovereignty over technology and information is its primary consideration. In Washington, the use of illicit cyber tools for illicit gain or intellectual theft by actors associated with China continues to be a problem area for American-Chinese cooperation. Painter mentioned the suspension of the China-U.S. working group in cyberspace. Nonetheless, he stressed that while dialogue is needed, American concerns regarding the aggressive use of cyber capabilities should be addressed first. On a broader scale, the United States has been pursuing cooperative initiatives with several Asia-Pacific states. This includes cooperation with states like Australia, New Zealand, South Korea, and Singapore. Painter highlighted the U.S.-Japan bilateral dialogue that includes all agencies which stresses the importance of formulating norms concerning cyberspace.

From a regional perspective, Painter then cited the work of the ASEAN Regional Forum (ARF) in promoting confidence building measures (CBMs). An upcoming workshop with the Singapore government was also mentioned to develop CBMs with other ASEAN states. He raised the issue of Internet governance; initiatives, such as the Internet Governance Forum (a multi-stakeholder forum for policy dialogue), were highlighted to illustrate the growing importance of multilateral forums. Some countries are looking for an increasing role for the International Telecommunications Union (ITU) but this is not good for security or the Internet. Although the ITU has an important role, there are better forums. In addition, an increasing amount of governments are recognising the multi-stakeholder approach as seen in the declaration made at the Net Mundial – Global Multi-stakeholder Meeting on the Future of Internet Governance. Painter also stressed how there is emerging consensus among experts that the United

Nations' espoused principle of universal human rights is applicable to the online realm. He mentioned that 27 governments are members of the Freedom Online Coalition.

Painter then discussed how to increase international stability through norms of state behaviour. He remarked how the 2013 UN Group of Governmental Experts (UN GGE) appeared to reach a consensus on the applicability of international law in cyberspace but how this applies is still being figured out. The UN GGE recognised that cyberspace is not lawless and as such precludes the use of proxies in cyber conflict, and it highlighted the importance of CBMs. There has been progress in the 2014/2015 report of the UN GGE. For instance, the UN Charter applies and some peacetime norms are affirmed such as: 1) to not attack critical infrastructure; 2) to not attack computer emergency response teams (CERTs); and 3) CERTs should only be used for defensive purposes rather than offensive. The U.S. would like to see that two further norms are agreed: 1) to respond to a state request; and 2) to not promote the theft of IP for commercial purposes.

In order to build transparency and confidence to prevent misunderstandings, Painter mentioned points of contact and the exchange of doctrine. For example, the OSCE has agreed to 11 voluntary CBMs and the ARF will hopefully bring this forward. The overarching principle to attain international security in the cyber domain is the push for greater transparency in the midst of emerging offensive cyber capabilities.

Painter concluded by pointing out how cyber foreign policy should consider not just threats but opportunities for cooperation. He exhorted states to build frameworks of response to common cyber threats. Moreover, cyber is important for developing countries to ensure their economic and social development. The growing salience of cyber issues will not slow down but Painter is optimistic that at least now, states are paying greater attention.

Contributed by Joseph Franco

Discussion

Painter was asked about the challenge of getting states to agree on applying international law to cyberspace. Painter remarked that the argument of applying the Law of Armed Conflict in cyberspace is synonymous to the militarisation of the cyber domain does not make sense. Another participant asked how best to promote change and innovation in cyber policy. The speaker explained that whole-of-government approaches work best, albeit at times such a multi-polar approach may appear chaotic. During the discussion, Painter also stressed that cultural differences are important, but they do not transcend international human rights. They should not be used as an argument to curtail access to information, as claiming total sovereignty over cyberspace runs contrary to human rights. A participant then asked about the degree of U.S.-China cooperation on cybercrime. Painter mentioned some initial links that had been established between the U.S. Department of Homeland Security and their Beijing counterparts. Specific measures include better information sharing between Chinese and American agencies and the increase of venues to interact. However, Painter explained that points of friction such as the alleged theft of intellectual property for commercial purposes needs to be addressed in order to achieve greater progress. He highlighted how media reports on purported illicit activities by the Chinese can diminish public and legislative support for further cooperative activities.

Contributed by Joseph Franco

PANEL 1:

Cyber and International Security: Opportunities and Challenges for Further Cooperation

Broadening Debates on International Peace and Security in Cyber

Wouter Jurgens, Head of International Cyber Policies, Security Policy Department, Ministry of Foreign Affairs, The Netherlands

Wouter Jurgens

Wouter Jurgens explained how the use of ICTs is a matter of strategic importance, and how all stakeholders – not only states – should have a place at the negotiating table on international issues. He posited that a free, open and secure Internet as well as the securing of rights is important. In addition, cyber is core to economic growth and innovation. He exhorted states not to suppress the open exchange of ideas in cyberspace.

In terms of international peace, Jurgens noted that cyber is an international issue that affects citizens all over the world. Jurgens argued that cyberspace brings new and unforeseen threats to states and that these issues need to be thought through. He raised two questions: 1) what is the role of cyber in international security; and 2) whether more can be done. Cyber tools are an instrument of power projection, and capabilities in the hands of both state and non-state actors are increasing rapidly globally. The proliferation of such tools is increasing instability. Jurgens noted that political cyber attacks are causing instability to the system, and he identified cyber as an area where states can be trapped in a security dilemma, in other words where defensive state capabilities can be easily mistaken as offensive cyber weapons.

Jurgens argued that cyber is not just a technical issue and it is increasingly a political problem that needs political solutions. He emphasised the need for states to look at the longer term to solve cyber issues. He advised that states acknowledge that there is a problem in cyberspace, given that some states refuse to acknowledge it; there is still time for the international community to do something before it becomes too late. He then stressed the need to deal with some pressing issues in cyber including: 1) attribution; 2) verification; 3) the inseparability of civilian-military infrastructure and how civilian infrastructure can be protected; 4) the uncertainty surrounding the cyber capabilities of other states; and 5) the need to ensure that security is not compromised as devices become more connected in the new Internet of Things (IoT).

Jurgens stressed the applicability of international law as well as the need to strengthen peacetime norms and CBMs. To this end, he praised the efforts of the UN GGE in creating a normative framework to limit threats and build confidence. Jurgens noted that the Global Conference on Cyber Space (GCCS 2015) contributed to the work of the UN GGE and furthered discussion on CBMs. While states have a central role, other parts of society should be part of the discussion. Further, more time is needed to both clarify and implement what has already been agreed. He does not necessarily advocate broader participation in the UN GGE but there is a need to create platforms to increase the presence of other stakeholders. In addition, he emphasised that the technology community should be consulted.

Jurgens further highlighted the need to understand what different states want in order to avoid a security dilemma situation. He warned though that this understanding may not be enough. He advised that the consequences should be highlighted before an attack takes place as a form of deterrence, and that cyber should be treated as a collective security problem.

He emphasised the need to cooperate with private corporations and regional organisations so as to build a broader consensus. He mentioned the important role for regional groupings such as the OSCE and ASEAN to lead on CBMs and norms since regional organisations are key to international level discussions. In addition, he suggested that the Global Commission on Internet Governance might be a useful model for solutions to negotiation platforms like the UN GGE. However a Helsinki process may not work as we should separate matters into baskets of issues.

Lastly, he argued for the need for more research on norms and CBMs. He promoted research-based policy advocacy and called for processes to be put in place to incentivise progress towards cyber issues. He warned that states should not be caught up in a security dilemma, and that cybersecurity should be seen as an important diplomatic challenge in its own right.

Contributed by Tan E Guang Eugene

Confidence Building Measures at Regional Level: What is New and on the Horizon

Yono Reksoprodjo, Expert Staff, National Desk for Information Resilience & Cyber Security, Coordinating Ministry for Politics, Legal, & Security Affairs, Republic of Indonesia

Yono Reksoprodjo

Yono Reksoprodjo observed that ASEAN is an entity based on confidence building measures, and the norms within the ASEAN community need to be respected. Reksoprodjo said that as early as 2009, ASEAN has been aware that proxy actors were active in cyberspace. He noted that some states conduct their cyber activities through direct proxies like China, but there were others that may conduct their cyber policies through indirect proxies.

He added that understanding the ASEAN culture is as important as international law, in dealing with outstanding disputes over physical spaces. He posited that culture plays an important role in regional relations, even with international law. Thus, he noted that the overemphasis on international law concepts will inevitably raise conflict, and these conflicts will also manifest in cyberspace.

Reksoprodjo explained that the building of both common understanding and common responsibility in ASEAN is a way forward. He expressed the need to find a balance between online freedom of expression and security in cyberspace, although this balance is not easy to achieve. In terms of international peace and stability, he espoused the need for the peaceful use of the Internet to maintain stability within states and to prevent the spread of radical ideology to improve security. Reksoprodjo also emphasised the need to equitably develop each state's capacity, so as to achieve CBMs among ASEAN states. He suggested holding joint simulations on a regular basis among states to test their capabilities and check their capacities to deal with crises. In reality however, he acknowledged that there are differences among states and much work remains to be done in ASEAN.

Reksoprodjo hoped that the ASEAN Regional Forum (ARF) workshop in Beijing in July 2015 could deal with CBMs. He noted that the international community at GCCS 2015 strongly promoted freedom and economic growth, and that there is a need to avoid the creation of a security paradox in cyberspace. He further stressed the importance of finding international and regional solutions for cyber through forums like the Shanghai Cooperation Organisation (SCO) and ASEAN in relation to other issues like terrorism and separatism. He further suggested that the ARF is a forum where potential solutions can be pushed, especially for countries like the U.S. and China.

Reksoprodjo emphasised the need for cooperation based on mutual trust and confidence. He suggested that bilateral talks are an important way to build consensus among states. He argued that there should

be a common understanding on non-interference in the domestic affairs of states and that this should be a leading principle. He further argued that the OSCE CBMs could be a guiding principle. International conventions on cyberspace governance should be held under the auspices of international agencies like the OSCE or NATO so as to foster cooperation and establish best practices in areas such as terrorism.

Reksoprodjo explained that there could be strategic alliances in combating cybercrime since it is an issue that affects all states. However, he cautioned that there needs to be a clear understanding of and distinction between cybercrime and cyber warfare. Further, he raised the issue of responsibility for failure in the system. He queried whether there are ways to build confidence in the system so as to prevent states from cheating.

Contributed by Tan E Guang Eugene

Redlines in Cyberspace – What the Sony Attack means for State Responses to Cyber Incidents

Tobias Feakin, Senior Analyst and Director, International Cyber Policy Centre, Australian Strategic Policy Institute

Tobias Feakin

Tobias Feakin noted that there have been an increasing number of cyber attacks in recent years, and spoke about the need to respond to these incidents proportionally. He spoke of the importance of good preparation and cooperation between governments, especially because of the increasing role of offensive capabilities.

Drawing on the experience of the SONY hack in December 2014 and various other incidents, he explained that states are under huge pressure to respond to cyber incidents. States are under pressure to strike back, often with cyber means, but this may not be the best response. He warned of the inadequacy and ineffectiveness of responses solely based in cyberspace. Nevertheless, designing timely, proportionate responses is complicated and policy responses have been ad hoc so far. Feakin thus argued for some level of preparation across different governments in the region to be done so as to decide the level of response to an incident. However, because of the use of criminal hackers and proxies, it is hard to pin down the originators of hacks and this frustrates efforts to assign responsibility for a cyber attack.

Feakin recognised the challenge of determining an appropriate policy response, but said it is not impossible. He suggested that responses will still largely be context dependent. However, he urged policy-makers to draw up a framework for guiding responses that consider three variables: 1) the severity of an incident; 2) the degree of confidence in attributing responsibility for the incident; and 3) consideration of the different response capabilities at the disposal of states.

He explained that the SONY hacks and the considerable damage sharpened interest in forming incident responses. SONY's response was entirely reactionary, and it was in Feakin's view, a damage limitation exercise that sought to control the release of information through legal gag orders. Feakin noted that SONY's reaction brought more reputational and financial harm to the company. In addition, it was only with the threat of 9/11 style attacks on American cinemas if SONY released its film, "The Interview", that the United States government stepped in. Sanctions were swiftly imposed on North Korea, demonstrating a proportional response that was open and taken by the United States.

Feakin then presented a list of criteria to develop a proportionate response framework, which included: 1) the physical damage caused; 2) the effect on society; 3) economic fallout; and 4) national interest. He further stressed that having such a framework is important for decision-making, and it could include other forms of policy responses such as diplomatic, economic and military responses. However, he warned of the limitations of action and called for patience in responding, particularly since digital forensics takes time and it is not always perfect. The possibility of using false

flags and other confusing factors cannot be ruled out.

Feakin suggested that the severity of the response be in proportion to the severity of the effects of the incident. He warned that a more severe response may carry political risks in itself. To conclude, he explained that having a response framework can provide a state with an idea of its capabilities so that it is not blind-sided should an incident occur. In addition, he suggested that government should also work with the private sector in gaining perspective on severity thresholds in different industries to form a response framework.

Contributed by Tan E Guang Eugene

Discussion

A series of questions were asked about the role of the UN GGE: 1) what is the role of the UN GGE and GCCS, and are some measures conflicting, some conciliatory; 2) how do these forums contribute toward confidence building; and 3) while both are necessary, though insufficient, could an ICT20 group be set up in addition to the G20. A speaker explained that the role of the UN GGE and the GCCS is to provide more avenues for discussion in ensuring peace and to contribute to the discourse rather than conduct adversarial negotiation. He noted that there can be many models or forums and there are two things that the UN GGE and the GCCS need to do: 1) not be a negotiating platform and interact with different stakeholders; and 2) make it as inclusive as possible. He explained that ideas were formed by research and there is a need to have multiple initiatives to initiate discussion at various levels such as at intergovernmental and academic level.

A participant commended the UN GGE's recent success in delineating the role of norms within cybersecurity and asked which aspects require the most attention currently. A speaker opined that one of the most contentious topics is the applicability of international law by states. For example, how should attacks below the threshold of armed conflict be classified? Another concern raised was how international law can be applied to non-state actors. A speaker suggested that states should have standing frameworks that delineate how they should address attacks that emanate from their territories.

A participant asked about a scenario where there is an absence of norms instead and about the viability of any effort at addressing cybersecurity issues. A speaker explained that there is still a need to strengthen the policies that pertain to cybersecurity concerns so that states would be able to communicate at the policy level. This would then encourage close cooperation in the intelligence community and with other countries. States should prioritise the establishment of norms.

A participant asked about states' adaptability to technology's dynamic changes since this may compromise policies already in place. A speaker suggested that this issue is not unique to the cyber domain. Conventions and laws should be forward looking and standards should be set internationally. This should be holistic and work should be done to garner support at the local, regional and international levels to keep up with defensive and offensive cyber capabilities available in countries in the future.

A participant asked about the regional readiness of ASEAN in terms of ICT and the ASEAN goal of being "cyber ready" by the end of 2015. A speaker explained that regional cooperation will help improve systems as a whole and it is a building block for international consensus. He further added that conferences and meetings give states the room to respond to cyber issues. Another participant added that ASEAN is very large and cybersecurity is being discussed in many ministries. For example, home affairs are implementing a targeted approach for cybercrime and the telecommunication ministries conduct cyber network exchanges across all countries. Nevertheless, the topics mainly focus on governance and crime.

A participant asked about trends in country responses. A speaker said that there is a lot of analysis on the state level but not as much as the individual level where most economic crime and investment happen. He raised an example of the nexus between software piracy and cybersecurity, and the inability of states to provide for the security of enterprises because the latest patches are not available to the mass market.

A participant asked how states should move forward beyond confidence building to more practical policies in the cybersecurity domain. A speaker replied that states must be clear as to what it is they are trying to achieve

through the confidence building process. For example, there is a need to redefine what the act of "retaliation" would entail in cyber warfare. This, according to the speaker, would require the clear delineation of norms and supplementary terms and conditions to set up procedures for rehabilitation or punishment within countries for the attacker.

A participant asked how ASEAN can deal with new cybersecurity issues that appear at the regional level. A speaker suggested that it is difficult to exclude CBMs within the region. Within ASEAN, states should study how to react to specific scenarios and to cooperate with each other. This would deepen trust levels and iron out standard operating procedures shared among the ten member countries. However, he cautioned that the term "confidence building" is often used loosely, and states should assess whether reaching out to other states is enough for confidence to be strengthened.

A participant mentioned that cybersecurity issues may be multifaceted, and asked the speaker for examples of impediments which may limit any addressing of cyber attacks. The speaker shared that it would be difficult to contain the spread of an attack if there are not many cybersecurity specialists to act quickly. The speaker also highlighted that countries should not separate cybersecurity from traditional security issues. He also felt that there is a lack of infrastructure within various countries to contain cyber attacks. He said that most agencies set up for this purpose may not enforce strict laws or punishments and they may even experience corruption within the agencies.

A participant asked about the regional nuances in applying a decision-making framework to state responses. A speaker explained that having a framework guides the decision-making process of the state and is not meant to be escalatory. He also suggested that the region needs transparency in capability sharing so that these frameworks can be meaningful, citing his experience in conducting red teaming exercises for the financial sector in the region. He said many countries without such frameworks could not deal with the escalation of crises during the exercise and would therefore be hard pressed to cooperate with other states in curbing crises.

A participant asked about the level of cybersecurity education of the end user in the region and whether this education can be improved. A speaker said that the education of the end user is very poor. Another participant suggested that the cost of anti-virus software, for example, can cost a lot of money in an impoverished region, and governments are limited in responses. He also asked whether the private sector could play a bigger role in improving cyber literacy.

A speaker asked participants whether a military response is necessary when critical infrastructure is destroyed following a cyber attack. A speaker suggested that it may depend on the importance of the infrastructure to the state. For example, the failure of financial infrastructure may constitute an attack on national security and warrant military attack.

The discussion then focused on the intense interdependencies which can be found within states as technology advances. Attacks on an interdependency linked to a main structure may bring the whole system down. There is then a need to protect the processes which ensure the functioning of the system. A speaker added that both the private sector and government have interests in safeguarding against cyber attacks. He suggested viewing issues from a "natural responsibility" perspective instead, which would suggest that different parties have a part to play in protecting a state's function and systems.

Contributed by Tan E Guang Eugene,
Romain Brian Quivooij and Joseph Franco

Panel 2:

SQUARING NATIONAL SECURITY AND DATA PRIVACY MATTERS

Managing Data Privacy and Civil Liberties Activities
Simon Chesterman, Dean, Faculty of Law, National University of Singapore

Simon Chesterman

Simon Chesterman first considered the inherent tension between rights of citizens and the security concerns of governments. Chesterman highlighted how privacy rights have become "eviscerated" by state activities. National security agencies, which previously looked at threats beyond their borders, are increasingly being tasked to help maintain internal security in the face of increasing incidents of political violence and terrorism. However, while there is strong opposition to mass surveillance by states, individuals are very permissive in sharing information on social media. This apparent contradiction appears to Chesterman as proof that the discourse between liberty and security is more nuanced than it appears. What he sees emerging is the shift towards a "data protection" paradigm rather than an all-encompassing privacy paradigm. He mentioned Singapore's Personal Data Protection Act as an example of future-proof legislation. Although, he explained that the legislation was originally intended in its drafting to be flexible, but flexibility can also mean uncertainties can arise.

He then discussed what role laws should play in ensuring citizen liberties. Consensus has yet to be attained in most countries on the normative (should law impose limits) and technical (could law impose limits) standards to be applied in limiting state power. Chesterman argued that specific national norms can find their way into global frameworks as a specific product gets rolled out internationally. For instance, Facebook's age limit regulations worldwide emanated from U.S. legislation covering the protection of minors. Another issue that often arises when the relationship between law and civil liberties is discussed is the issue of jurisdiction - which has become more complex as data storage has increasingly become de-territorialised. The importance of jurisdiction and territoriality has always been considered by Singapore, with cyber-related legislation attractive for firms engaged in providing big data solutions.

Given the nascent nature of legal protections, Chesterman highlighted how citizens have taken it upon themselves to protect themselves. He also mentioned that in Europe, there is much discussion over demands of citizens for the "right to be forgotten". While the motive for such advocacy is rooted in libertarian ideals, it remains liable to misuse. For instance, Chesterman illustrated how the right to forget could be used by sex offenders to obscure their judicially imposed listing in public registries. Another issue that emerges during discussions on self-help is how privacy is being viewed now as a luxury to invest in. Chesterman shared how some institutions in Europe are considering investments in quantum cryptography to guard against snooping by the NSA.

In conclusion, Chesterman tried to paint a picture of the future of liberties and privacy. He predicts that corporations will continue to be the major players in managing the information of individuals in cyberspace. Thus, limits to state power will not come from laws and government but from private corporations.

Contributed by Joseph Franco

Cybersecurity and the Balancing of National Security with Data Privacy and Freedom of Expression – the Philippines Perspective

Geronimo L Sy, Assistant Secretary, Department of Justice, The Philippines

Geronimo Sy presented a legal framework that highlights the nuances between cybersecurity and cybercrime in the Philippines. For Sy, cybercrime is a phenomenon within the bounds of criminal law and thus not a completely novel challenge. Nonetheless, he pointed out that the imperatives of criminal law on evidence collection may be at odds with national security considerations. Consequently, the right of the Philippine state to collect data could have friction with civil liberties. This is a potentially contentious issue in the Philippines as civil liberties are deemed an inseparable component of individual rights.

He then explained how laws have evolved in the Philippines to account for the challenges posed by the cyber domain. Sy underscored how change is largely incremental, with no specific coherent process. It was during the 2000-2015 period that Philippine legislators began to enact specific laws to cover technical aspects such as cybercrime. Until the present, Sy recognised that while laws change incrementally, technology shifts are disruptive - with the former playing catch-up. It was only in 2015 that the Philippine government released a Cybercrime Report based on year-end information from 2014.

Sy then focused on the challenges faced by the Philippines to attain cybersecurity. First, there is a disjointed interface between stakeholders tasked with legislation, such as lawyers/legislators, and the technical community for cybersecurity. Second, there is a lack of capacity and capability to pursue cybersecurity initiatives such as securing the proper tools and retaining talented personnel. Third, public engagement remains limited. Sy contrasted how citizens were in consensus over the threat posed by cybercrime but remain sceptical over cybersecurity initiatives. Discussions over cybersecurity degenerate into accusations of government censorship and intolerance for dissent. Finally, Sy highlighted how there remain limited methods to reliably assess the effectiveness of plans executed by Philippine ministries.

Sy then shared some recent developments in the Philippines with significant impact on cybersecurity. The Philippines' 2012 Cybercrime Prevention Act has recently been given more teeth with the crafting of its Implementing Rules and Regulations. Sy stressed the importance of cooperative initiatives with other states when he talked about the establishment of "cybercrime desks" by Philippine law enforcement agencies. These desks are tasked as points of contact for processing and acting upon requests for mutual legal assistance. He highlighted the ongoing initiatives by the judiciary to create around 20 to 30 "e-courts" tasked to hear cybercrime cases. Within the Philippines' Department of Justice, Sy also referred to the establishment of its own Cybersecurity Incident Response Team (CSIRT).

Overall, Sy's presentation underlined how changes in Manila's cybersecurity policy will continue to progress at an incremental pace.

Contributed by Joseph Franco

Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective

Bryan Tan, Partner, Pinsent Masons MPillay LLP, Singapore

Bryan Tan

Bryan Tan mapped out Singapore's experience and perspective on cyber issues. Policymakers have recognised that national security is no longer limited to the physical realm. Today's cyber criminals are "submarine threats" that lurk within systems, patiently waiting for the right time to strike. Tan asserted that the days of bank robbers are long past, with cyber criminals able to achieve illicit financial gain with minimal physical

risks. It is in this changing environment that Singapore's critical information structure exists.

The importance of Singapore's cyber infrastructure to its prosperity is manifest in the constant changes to its legal environment. Tan recalled how successive changes to the 1993 Computer Misuse and Cybersecurity Act have reflected the intent to harden the country's information infrastructure. Another key facet of the cyber-related laws in Singapore is to reiterate how freedom of speech is a qualified right, even in cyberspace.

Tan then talked about the experience of Southeast Asian states in cybersecurity. ASEAN has been active in pushing cooperative activities. He cited the salience of cybercrime and cybersecurity in discussions at ASEAN Ministerial Meetings and the ARF. Outside of these multilateral mechanisms, Tan referenced three outlying issues of great concern to governments.

First, governments in Southeast Asia remain keen in having ensured access to encryption standards operated by private corporations. Tan remarked how different countries have different notions of individual rights - with the debates far from reaching a consensus. Next, governments are becoming more assertive in demanding for greater localisation of information collected from citizens. Legislation and regulation increasingly seek to have information stored in local data servers, to prevent the exfiltration of citizens' information from national borders. Finally, Tan shared how some governments have expressed the desire to create government-only networks to minimise dependence on the commercial backbone of cyberspace. However, requirements for local manufacturing of technology and government networks may have an impact on commercial services.

Tan then discussed the impact of national security needs on creativity and innovation as well as the digital economy. He argued that restrictions to both the production and consumption of information can stifle creativity. National security restrictions should not be too overbearing at the expense of innovation. Instead, Tan called for the emergence of a less contentious paradigm to balance both factors. In Singapore, for instance, the country is trying to spur innovation and it should be a leader in the region in terms of the start-up economy. Creativity, he stressed, is as important as safety and should not be viewed as a zero-sum contest.

Contributed by Joseph Franco

Q&A Session

A participant asked to what extent is the right to be forgotten a Euro-centric phenomenon. A speaker remarked how the EU has traditionally been a strong advocate for human rights and privacy. This may clash with the freedom of speech principles adhered to by American society, which in turn provide the foundations of Internet firms like Google. Another speaker stressed that individuals should be aware that privacy is not synonymous with data protection as the former assumes the creation of a bubble to stop the collection of data. It would be more productive to instead aspire for data protection - the management of data broadcasted by an individual. A participant then asked about Singapore's approach to Internet governance. In response, it was pointed out that the city-state follows a multi-stakeholder approach. However, in terms of the Government ensuring that the Internet is not misused, it will step in if required but will not necessarily explicitly state why. The government would want to exercise a "light touch". A question was asked about the legality of private encryption capabilities. It was pointed out that Singapore does not ban products solely on the basis of encryption strength. Singapore is a small country and if there is a product that has specialised encryption, it does not necessarily have the economies of scale to entice firms to change their product in contrast to the larger market share they control in other countries. This was followed by an explanation by a speaker that in some countries, like the Philippines (although this has not been tested yet), a "good faith" defence might be acceptable to rationalise the sale of encryption. Nonetheless, if a specific product is used for a crime, existing statutes can be used to charge perpetrators for obstruction of justice charges.

Contributed by Joseph Franco

Panel 3:

DIGITAL ECONOMY

Public-Private Partnerships from an Industry Perspective

Jan Neutze, Director of Cybersecurity Policy, Microsoft EMEA

Jan Neutze

Jan Neutze explained how public-private partnerships (PPPs) are essential to cybersecurity, and highlighted that such partnerships are constantly changing. He touched on the key trends in these partnerships and how the nature of these partnerships is evolving.

Neutze made clear that government has an important role in risk management. He emphasised the crucial role of exchanging information with private companies to establish and strengthen a bi-directional relationship, especially with critical infrastructure providers for example. He raised the issue of dealing with vulnerabilities in terms of reporting them to vendors rather than stockpiling to potentially use for national security purposes. He suggested that government could increase training to educate the private sector on how governments deal with ICT and its vulnerabilities. Further, the private sector can also drive action on government policies both domestically and internationally. He further recommended information sharing by adopting a voluntary framework, and provided examples on the types of information shared in a bi-directional relationship such as, incidents or threats on regional and local levels, information on vulnerabilities, and situational awareness. He added that increased communication with various stakeholders between governments and the private sector will result in closer coordination and the dissemination of best practices.

Neutze then provided some recommendations to foster closer relations in PPPs. He stressed that relevant information should be disseminated to the proper stakeholders, and situational awareness should be adopted in the sharing of information. Information sharing on actionable threats could potentially identify vulnerabilities in ICT systems. Neutze also highlighted that governments could consider the implementation of a mandatory framework. And patience is needed in evaluating the root cause of an incident as it takes months of analysis during the post-incident process.

Neutze shared examples of existing PPPs, such as: 1) the Cybersecurity Awareness Alliance in Singapore, which was established in 2008; 2) the Alliance for Cybersecurity in Germany, which comprises government and the Association for Information and Communications Technology; 3) the National Cybersecurity Centre in The Netherlands, which launched a Memorandum of Understanding with neighbouring countries; and 4) Tech UK. There has been significant maturing in the public-private partnership sector, but there is still much to develop over time. For instance, only five of the 28 EU Member States have implemented PPPs.

Neutze highlighted the changing nature of the Internet, and mentioned that the projected number of Internet users in 2025 shows significantly more users in China than the EU and U.S. combined. There is also room to grow for expanding the number of users in India and Indonesia. Moreover, the Internet landscape is changing as more people are connected to the Internet through smart devices, with 50 billion connected devices worldwide.

Emerging differences involving global cybersecurity commitment need to be refined, especially in policy implementation and maturity levels of cybersecurity. Cybersecurity priorities for EU Member States include the establishment and enhancement of cybersecurity frameworks such as the Network and Information

Security (NIS) Directive. Methods such as cybersecurity baseline measures, mandatory reporting schemes, and audits are harmonised across the EU, and this Directive could be used by other regions to draw lessons. Neutze urged for the comparison of a risk-based versus compliance focus, and for the effective application of limited resources and capabilities.

In addition, he explained that the President of the United States recently issued an Executive Order calling for the improvement and protection of critical infrastructure and cybersecurity. The NIST cybersecurity framework involves commitment and engagement from stakeholders on a voluntary basis. This is effective as the input from key stakeholders, coupled with the leveraging of government procurement, enables security products to meet harmonised security standards. This encompasses three areas, namely: 1) government procurement; 2) private sector risk management; and 3) cybersecurity regulation.

He posited that the government's role in a changing global landscape is crucial given the increase in offensive and defensive technology and capabilities over the years. Data access should be part of the law enforcement mandate, and emerging regulations should be well-tailored and defined. Lastly, he provided insight from a December 2014 study by Microsoft on the types of norms that are needed from the corporation's perspective which is fundamental to effective PPPs.

Contributed by Dymples Leong Suying

Securing and Optimising the Next Wave of Innovation in Smart Cities

Michael Mylrea, Chief Information Security Officer, Cyber Innovation Development

Michael Mylrea

Michael Mylrea defined a smart city as one that brings together technology, governments and society to enable the following characteristics: (1) a smart economy; (2) a smart environment; (3) smart living; (4) smart mobility; and (5) smart people. He cited Singapore as a success story in building a cyber-smart nation, and noted other examples of smart cities such as Brazil's City Coordination Centre, which centralises 30 different government departments, companies and utilities. He also noted New York City's Microsoft Domain Awareness System, with real-time analysis of public safety data.

Mylrea stated that smart cities are facing new threats such as digitisation in the networking of critical infrastructure that could expose vulnerabilities, with software glitches resulting in massive amounts of data being hacked and exposed. Factors such as energy, environment and rapidly growing population are challenges that are complex, non-linear and rapidly evolving in nature. He emphasised that the survival of all modern organisations are dependent on them being both "cyber and energy organisations". Digitisation now connects all other critical infrastructures, creating opportunities as well as exposing vulnerabilities. He highlighted that smart cities can increase the risks of cyber attacks in areas such as power grids, transportation, and utilities. Mylrea gave examples of recent cyber attacks like the Night Dragon cyber attack and the 2011 Stuxnet virus attack. He stressed that compliance by companies to cybersecurity frameworks does not guarantee immunity from vulnerabilities in smart building controls and

automation systems. In particular, he drew specific attention to a hacking incident at a large U.S. retailer through the smart building control systems. What was particularly interesting in this case was that the company had complied with standards. Mylrea then suggested that compliance with standards does not necessarily involve securing smart building controls and building automation systems.

Mylrea highlighted that energy infrastructures are increasingly digitised and connected to cyberspace. The industrialisation of networking control systems is a cause for concern in the future. Cybersecurity must be built in the design criteria and can no longer be an afterthought in the design process. Training and education is crucially important. He suggested implementing approaches such as standard operating procedures, monitoring of staff and inventory. He also recommended delving into cybersecurity maturity models for the identification of securing infrastructure, such as the Department of Energy's cybersecurity maturity model, which considers which critical infrastructure needs to be secured. Another example of this is an Asia Pacific Economic Cooperation's (APEC) cyber energy nexus study that examines the 21 APEC economies in their efforts to secure energy structures and identify the challenges faced.

Opportunities for cybersecurity abound, such as energy smart technology which transmits data and information to utility companies, providing regular updates. Another example involves smart wind farms that send engineers GPS coordinates when the wind farms are due for repair. Mylrea pointed out that the world has experienced two waves of innovation, namely the industrial revolution and the Internet revolution. He mentioned that the world is now on the cusp of a third innovation wave, which will combine cyber and energy technology from the first two waves to develop new game-changing technology.

Mylrea commented that the advent of new, game-changing technology will drastically change cities, skillsets and jobs. He called for higher investments in smart grid technology, especially in Southeast Asia. To conclude, he emphasised that cybersecurity policy and solutions should continue to remain smart and holistic in the development of smart cities for the future.

Contributed by Dymples Leong Suying

The Economic Security Implications of Cybersecurity
Daniel Castro, Vice President, Information Technology & Innovation Foundation

Daniel Castro

Daniel Castro observed that cybersecurity is increasingly important as countries are still being exposed to vulnerabilities and risks, with key fundamental problems still unfixed. He made note of the recent high profile hacks in the private sector, which revealed the underinvestment of cybersecurity measures by companies. Governments can ill afford to leave the private sector to deal with such challenges alone; partnerships are beneficial for both the public and private sectors.

Castro commented that the current focus on national security overshadows the economic implications of cybersecurity. He added that policy has been misguided, economic considerations have not been front and centre in the debate, and that a balance must be struck. Policymakers need to realise that cybersecurity decisions have substantial economic impacts as the economic costs of such vulnerabilities are hugely substantial. In addition, he recommended that trade and commerce representatives should participate as significant stakeholders in these cybersecurity discussions.

Economic implications are not being considered across the globe and there is not enough focus on trade implications. Economic interests are also used to support protectionist policies such as data storage within countries; the manufacturing of products domestically; China's security laws; India's preferred market access strategy; Russia's data localisation requirements; and U.S. policy on procurement. Further, following the Snowden revelations, it is crucial to

ensure the protection of citizens' right to privacy. Thus, he stressed that it is important that countries agree on strong mechanisms to promote ethical cyber behaviour. The rise of trade barriers for foreign companies can raise costs for imports of ICT products and can also affect the quality of products.

Castro provided four recommendations: (1) recognise economic consequences by acknowledging that public agencies are not immune to cyber vulnerabilities; (2) thinking about how we re-orient government strategies in cybersecurity, as vulnerabilities are rarely shared within the cybersecurity industry. Coordination between government researchers and the private sector to eliminate such vulnerabilities and sharing of best practices should be encouraged; (3) new ways to restore trust between countries by thinking of methods to enable hardware and software to be more secure, and getting countries to agree on international means of testing and mechanisms to discourage bad behaviour; and (4) the involvement of relevant stakeholder groups such as technocrats who have necessary expertise in the areas of Internet governance and cybersecurity.

Contributed by Dymples Leong Suying

Discussion

A speaker explained that the challenges of risk management will continue to be part of the operating field, with risk evaluation being the largest factor. Risk management will continue to evolve and become highly complex. Providing different control settings can enable organisations to map their maturity levels and act accordingly. It was mentioned that the EU NIS directive could enable the EU to develop a framework by implementing cybersecurity baselines. It was also noted that striking a balance between the dynamics of economic interests and cybersecurity is of the utmost importance.

The role of governments in cybersecurity was discussed, including whether governments should incentivise companies to adopt best practices. The focus for companies is growth and expansion, and many deem the steep cost of implementing cybersecurity processes as a deterrent. Governments should ensure that help is granted to SMEs to ensure that cybersecurity processes are implemented correctly, by keeping processes simple and transparent. Government should also consider ways to break down barriers of cybersecurity procurement and educational efforts to increase technical competencies. It was noted that little has been written in the areas of cybersecurity, organisational change and leadership in academia, and cybersecurity education could be incorporated in MBA curriculums for c-suite leaders.

On the issue of the significant Internet penetration rate in China and its impact on cyber norms, it was noted that the evident growth of ICT users will result in a major role for the country in international conversations in areas such as governance and cybersecurity concerns. A speaker mentioned that in the absence of norms, it could raise deep concerns if the government is left unchecked by the private sector and academia.

Regarding PPPs, it was noted that this is still at a nascent stage in Singapore. It was suggested that education and training in cybersecurity should also be encouraged within the society, to ensure sufficient security awareness.

A participant asked whether public and private partners can work more effectively to address cybersecurity issues. A speaker explained that both the public and private parties must agree on similar objectives. One concern which public organisations largely face is how to ensure the convergence of interests in both the public and private sectors, and how to prevent any malpractice by private contractors. Regulatory measures such as risk assessment exercises and the evaluation of project proposals, which public organisations can utilise before and during the duration of any cybersecurity project, were suggested. Another concern which private companies may face is that PPPs may favour larger private companies and exclude the smaller ones. However, it was considered an unfair argument since securing the cyber domains may not necessarily require large manpower or capital; smaller companies should also be given the opportunity for public-private partnership.

As some participants cited the challenges of overcoming mistrust and establishing relationships of trust, a speaker emphasised the respective roles of the public and private sectors. Drawing a parallel with the

theory of policy-making, he explained that the latter is traditionally based on the nexus between a problem, a solution and an opportunity. By contrast, cybersecurity problems exist, but solutions remain uncertain. He went on to mention that the fears of a digital Pearl Harbour or Cyber 9/11 were unfounded, since low and medium cyber attacks are dominant. He stressed the valuable role of the private sector as a driving force in providing cybersecurity solutions.

Asked about the diversity of countries' stances on the Internet, a speaker raised the possibility of a sufficient number of smart countries speaking with one voice. He recalled that the U.S. and China initiated an ad hoc collaboration on spam in the early 2000s. Despite shared scepticism, both parties quickly realised that they encountered the same problems and had similar perspectives. In light of this example, a key question is to determine whether or not some forums of cooperation can be improved or even replaced by other, more efficient forms of collaboration.

A participant asked about the importance of education in cybersecurity issues for the general public. A speaker agreed that there is an intense need for education as very few individuals prioritise cybersecurity. He offered that there is minimal literature on cybersecurity leadership and awareness, and that many enterprises are unaware of how important it is to securitise computers. There is a need for lifelong cybersecurity education and short- to mid-term programmes to educate individuals on the benefits of securing their software. Deeper analysis should also be taken to understand how people may react to threats, or why individuals refuse to attend to cybersecurity in the first place.

Another participant asked if cybersecurity should be part of corporate social responsibility, and a speaker suggested that this should be encouraged. Companies should emphasise the fact that companies' bottom-line are dependent on their cyber domains, and that every employee has a responsibility to safeguard company software and equipment. Governments too should encourage this form of corporate social responsibility in the public domain, and develop innovative methods to accomplish it.

A speaker shared how cities can benefit from being smart cities despite heightened cybersecurity concerns today. One benefit is that smart cities may overcome many of the cities' limitations by offering alternative solutions to current problems. It is beyond just conforming to a global trend in transforming cities into technologically integrated locales, but also empowering more citizen participation in deciding how they might want to utilise technology in their daily living. He added that there is no benchmark when measuring smart cities, but offered Barcelona as a suitable example of a city moving towards innovative and beneficial use of technology for its inhabitants.

Asked if the process of securisation of smart cities relied on a holistic or segmented approach, a speaker stressed the combination of both perspectives. He explained that the protection of most critical energy-cyber assets is a priority in the U.S. in order to make the most productive use of limited resources. A participant asked about the nature of a potential worst-case scenario in this regard. A speaker explained that entire networks had been digitised in the United States and this entails huge interdependencies with a potential snow-ball effect that could lead to massive disruption (as illustrated by the Northeast blackout of 2003). Situation awareness was described as a key element of crisis management.

Another participant asked about the smart capabilities of developing countries. The speaker emphasised that the latter have a strategic advantage as they are in a position to assess the past successes and failures of developed countries, especially in the field of cybersecurity. Describing the result of his research across the APEC economies, he noted that many had deployed smart technologies prior to implementing cybersecurity systems.

A participant asked whether the responsibility to improve PPPs should depend on the government or the private sector. A speaker replied that both have a key role to play. He stressed that PPPs should not be seen as an ideal mechanism for collaboration, and that mutually beneficial information-sharing between the public and private sectors needs to be improved. The role of Microsoft's trustworthy computing initiative launched by Bill Gates in 2002 was discussed - all Microsoft products had to undergo extensive security review testing, including a security development life cycle which has since become a leading methodology.

A participant enquired about the potential role of the private sector in overseeing cybersecurity issues pertaining to national security. A speaker recalled that 89% of the Internet infrastructure is owned, operated, developed and maintained by the private sector. To a large extent, the situation is the same for critical infrastructure services such as the management of water, electricity and transport systems. PPPs act as a useful tool of collaboration in the field of cybersecurity, but the shaping of these partnerships need to be further defined.

Contributed by Dymples Leong Suying, Romain Brian Quivooij and Joseph Franco

KEYNOTE ADDRESS

Cybersecurity Trends and Issues from a Singapore Perspective

John Yong, Director, Infocomm Security Group, Infocomm Development Authority of Singapore

John Yong

John Yong underlined the need for Singapore to become a smart nation. To make the city-state more efficient for its inhabitants, natural and human constraints such as a small territory and high population density must be turned into advantages. In addition, the growing importance of health and support services related to senior citizens makes this smart evolution necessary.

The openness and receptiveness of Singaporeans to technological developments provides fertile ground for the implementation of innovations. Yong stressed the importance of data analytics for more effective decision-making and planning. He referred to the commoditisation of hardware as a future major trend that will need to be taken into account, and emphasised the key role of digitisation in the smart process.

The development of ICTs to their fullest potential was said to be a central element in the international competition pitting Singapore against larger countries. In this context, the example of Estonia was used to illustrate some of the challenges and opportunities faced by Singapore, as Tallinn is resolutely committed to advancing along the digital road. Among the wide range of projects aimed at improving people's quality of life, initiatives such as universal Wi-Fi access, smart dispensary systems and autonomous vehicles are feasible. However, the full safety of users currently remains uncertain in the latter case. An important challenge is combining quality and security, as one without the other is not acceptable.

Singapore's high level of connectedness reflects a technological success but it also raises cybersecurity challenges, some of which are related to big data and a complex user-environment. Yong referred to data privacy as an important security concern for the Government, as the privacy of citizens' data that is collected by any digital device needs to be protected. Citing the increasing number of cybersecurity incidents at the global level, he explained that the potentially high number of unreported cases could result in misleading figures. Other threats of particular concern include defacement; disruption; data breach; corporate espionage, and financial loss. If not handled properly with a minimal level of cyber-hygiene, some of these risks could seriously affect any organisation and entail significant costs such as reputational damage. Major cyber threats anticipated in the next few years will involve increased number of data breaches; evolved forms of DDOS attacks, and targeted authentification-based attacks.

Yong evoked the three cybersecurity steps of prevention, detection and recovery, and described some of the major initiatives taken by Singaporean authorities in this domain. These include the launching of a secure and resilient Internet infrastructure code of practice; the appointment of a chief information security officer, and the setting up of a Monitoring and Operations Command Centre to enhance the ability to manage incidents and situations that may pose an imminent threat across government and public telecommunications infrastructure. To conclude, Yong characterised the three dimensions of design, pervasiveness and adaptiveness as key components of a cybersecurity programme.

Contributed by Romain Brian Quivooij

Q&A Session

A participant asked if Singaporean authorities had already caught the perpetrators of defacement, and if the city-state had the necessary technological and legal tools to combat this threat. Yong explained that Singapore is probably a very attractive target for defacement. The latter should be understood as a failure of the ICT system, which is not systematically the result of a malicious intent. Among the range of responses available, Yong recalled that it is essential to check one's system on a regular basis so as to identify defacement in proper time. He described the reliance on other means of communication as a good user practice, and stressed the crucial need to restore the website targeted by a defacement attack as soon as possible. Another participant enquired about the nature of smart innovations applied in Singapore. Yong referred to autonomous vehicles to illustrate the potentially high impact of smart initiatives on citizens' lives. As safety remains a paramount consideration, cybersecurity is intended to play a major role in the architecture of a smart nation.

Contributed by Romain Brian Quivooij

Panel 4:

CYBER IN PRACTICE – KEY DEVELOPMENTS

The Fight against Cybercrime and Cybersecurity: How to Converge in a More Efficient Way?
Christophe Durand, Head of Cyber Strategy, Strategy & Outreach, Cyber Innovation and Outreach Directorate, INTERPOL Global Complex for Innovation

Christophe Durand

Christophe Durand discussed INTERPOL's approach in tackling cybercrime. He provided an overview of INTERPOL's framework of operations, followed by a detailed introduction into efforts taken by the global law enforcement organisation in dealing with cybercrime incidents. The presentation concluded with recommendations to harmonise global approaches against cybercrime.

Describing the INTERPOL framework as an old idea with a modern impact, Durand highlighted the organisation's interconnected presence worldwide. With 190 member countries, INTERPOL is the world's largest police organisation, providing a networked and uninterrupted source of support for national police organisations worldwide. The main aim of the organisation is to facilitate international police cooperation to effectively trace crime and criminals across borders.

Cybersecurity approaches dictate a focus on protection of the integrity of IT systems, and ensuring the resilience of the system by putting effective recovery and continuity processes in place. This may seem removed from the approaches in combating cybercrime, which involves the detection, attribution, and disruption of cyber-criminal networks. Where business and the private sector tend to be concerned about the former, law enforcement agencies are more focused on the latter. For Durand, both areas converge together as security is never 100 per cent guaranteed, and depends greatly on effective police investigations in dealing with cybercrime. Noting in particular the difficulties of attribution, Durand suggested the need for a "forensic by design" approach in investigating cyber breaches, which requires close cooperation between investigators and the victim of the crime.

The need for greater cooperation is clear, given the borderless nature of cybercrime networks. Hence, there should be an emphasis on harmonisation of processes and laws that govern this area and for more efficient rules to deal with cybercrimes. INTERPOL has been focusing on the means for coordinating and enhancing cooperation around the world, including working together with other organisations such as companies in the private sector and universities. An example is the development by INTERPOL of a Darknet monitor for research purposes, which can be used to identify methods and strategies used by cyber-criminal networks. This focused training course and others like it will remain essential in fostering cooperation across law enforcement agencies, the private sector, universities and research institutes as well as provide opportunities to enhance knowledge and disseminate ways of tackling cybercrime. To conclude, Durand highlighted that one of the main challenges remains the level of skilled human resources available to support cybersecurity initiatives.

Contributed by Yeap Su Yin

The Strategic Approach of the EU to Cybersecurity and Defence

Wolfgang Roehrig, Programme Manager & Project Officer, Cyber Defence, European Defence Agency

Wolfgang Roehrig

Wolfgang Roehrig's presentation provided a detailed introduction to the strategic approaches adopted by the EU in developing cyber defence capabilities. The presentation covered the following: (1) an overview of the work undertaken by the European Defence Agency (EDA) in the area of cyber defence; (2) the political and strategic frameworks in place to manage cybersecurity in the EU; (3) examples of cyber initiatives taken by small countries in the EU; and (4) conclusions that can be drawn from current approaches.

The role of the EDA is to support the capabilities development of member states. From a European perspective, the respective militaries are increasingly dependent on civilian critical infrastructure which is becoming more network-enabled. There is also more reliance on commercial products, with exposure to the same vulnerabilities faced by civilians and the private sector. Critical military functions are becoming increasingly cyber-enabled. Further, there are variations among member states in terms of cyber capabilities, as well as a lack of a common minimum standard in ensuring cyber preparedness.

In terms of the political and strategic framework for managing cybersecurity, the conclusion of the European Cyber Security Strategy in February 2013 represented a successful joint enterprise by member states in coming to an agreement and managing areas which are usually addressed at the national level. In November 2014, the EU Cyber Defence Policy Framework was concluded, synchronising perspectives on cybersecurity and cyber defence from a military perspective. Further, an important aspect from the military perspective has been the fostering of civil-military dialogue, with a high potential for fostering cooperation in the cyber domain.

Across the 28 member states, managing cyber strategies at both the EU and national levels is a complex matter. In coming to successful conclusions on such joint frameworks, consideration was given to the fact that most member states already had their own national strategy for cybersecurity or were in the process of developing one. Further, from a military perspective, member states ranged along a continuum of two extremes in terms of military strategic approaches. On one side, there are countries which adopt a closely integrated civil and military approach, such as the Scandinavian countries. While at the other extreme, there are those that practise a loose coordination between the civil and military sectors, such as Germany. As such, it is necessary to find a middle ground in which to foster cooperation between member states, so as to ensure that all stakeholders feel comfortable in dealing with each other.

He then highlighted the ENISA guide to support national strategies, and described some work of the EDA Project Team Cyber Defence such as a pilot strategic decision-making course and exercises on cyber defence. The Estonia-Latvia Presidency Cyber Hygiene Initiative signed in May 2015 is another example of an important initiative by two small member states. This initiative raises awareness of and promotes the need for basic cybersecurity standards within defence organisations covering human-related risk factors, which has been a factor in more than 80 percent of cyber incidents reported.

Roehrig then explained that there are advantages and disadvantages when it comes to cooperation between small and large countries. While, in general, cooperation is a must, small countries will have to be cognisant of the fact that the resources they have are limited in comparison. In addition, cooperation with countries that are of the same size is potentially valuable as both usually share the same requirements.

In conclusion, Roehrig pointed out that while there has been much achievement during the last three to four years, one area that needs more attention is in ensuring that there is a sufficiently sized, skilled workforce to carry out the various cyber initiatives. He emphasised the need for cooperation and trust, notwithstanding the sensitive nature of the issues involved.

Contributed by Yeap Su Yin

Intelligence Gathering and Analysis in Cyberspace
Eugene Teo, Senior Manager, Symantec Security Response, Symantec Asia Pacific

Eugene Teo

Eugene Teo highlighted the role of PPPs in managing cyber attacks. He outlined the sources available, both publicly and privately, on cybercrimes and attacks as well as examples of cooperation between different sectors such as sharing information as well as solutions to prevent and combat such crimes. He concluded by pressing for more effort to achieve an overarching framework that would encourage a more dynamic information-sharing environment, with time-sensitive information disseminated quickly to relevant parties across the public and private sectors.

Many software security companies such as Symantec operate with teams that deal with customer escalations of issues concerning the security of their networks. This serves two purposes: 1) to provide protection for users of the company's software; and 2) to collect information for monitoring and investigation purposes. Other than this, such companies would also have dedicated staff or teams that monitor incidents, threats and espionage, which may not originate from the company's customers or existing users. These incidents which occur on a global scale, are tracked with the aim of collecting data on incidents such as spam, malicious files or traffic, and malware. Close cooperation with network providers, ISPs and data centres is beneficial. These organisations may at times provide access to IP addresses used by criminals in order to track and monitor the situation.

Teo noted that there are many good sources of information on cyber attacks that can be accessed by the public. An example is that of CERT-EU, a website which carries good sources of information. While there are many publicly available sources, many private advisories are not accessible by the public as information is passed from government to government. Among security and software vendors and industry, there are also networks of information that are kept private from the public - these networks tend to have stringent membership requirements, requiring new members to be introduced by existing ones.

In terms of PPPs, Teo noted that from the private sector perspective, there is an underlying understanding of the necessity to provide timely information to help the authorities keep a check on cybercrime networks and for the authorities to provide protection from potential threats. In terms of the public sector, the need to cooperate in sharing information has also taken root. An example would be actions taken by the FBI which has set up an alert system to provide notification to private industries on a regular basis. While the information passed tends to be in the form of a vague summary of the attack, important details are passed to ensure that companies can take steps to mitigate or discover whether their systems have been breached.

In conclusion, Teo noted that there is a need to enhance processes that would create a more dynamic information-sharing environment, with time-sensitive information disseminated quickly to relevant parties across the public and private sectors. In particular, governments need to play an active role in formulating a neutral framework where different stakeholders can come together and share the information that is needed to combat cybercrime.

Contributed by Yeap Su Yin

Discussion

A participant asked whether private companies should take the lead in PPPs when dealing with cybercrimes as they often have innovative solutions. A speaker noted that this is not necessarily the case as many public organisations are also able to come up with innovations solutions. However, they are not able to commercialise such solutions. In terms of such partnerships, a speaker opined that governments should take the lead as most companies operate with the objective of making a profit. Governments, on the other hand, can provide a neutral and independent framework in order to drive such partnerships. A participant then asked about steps being taken to ensure the sustainability of a skilled workforce in the cyber industry. A speaker explained that currently there is stiff competition between the private and public sectors when recruiting enough staff to manage their operations. Private companies have also begun to invest in R&D centres which can train their staff in the requisite skills. Further, they are working with universities in designing course content that would ensure that graduates have the requisite skills and knowledge that are useful to the industry.

A participant enquired about information-sharing between EU Member States. A speaker noted that there are different trust levels among the Member States and more needs to be done to foster mechanisms that would encourage the formal sharing of relevant information. A participant asked whether the EU is now better prepared for a cyber attack such as the incident in Estonia in 2007, and if so, what would be a response. A speaker replied that following the incident in Estonia, the Member States have made comprehensive attempts to identify lessons. Better crisis management mechanisms have been put in place to respond to such eventualities. A question was then posed concerning the need to manage both the online as well as offline consequences of a cyber attack. A speaker explained that the crisis management mechanism established for a cyber crisis so far was mainly driven by offline incidents, such as the volcanic outbreak in Iceland in 2010. He agreed that cyber incidents will always be accompanied by incidents in the physical domain or it could transpire that the consequences of a cyber attack have ramifications in the physical world. Hence, it would be prudent to ensure that response mechanisms be designed to manage both online as well as offline consequences.

A participant asked for more information about international cooperation for European countries and whether there are examples of cooperation with specific countries outside Europe. In particular, the participant was interested in whether there are any specific areas where more work needs to be done. A speaker explained that cases of international cooperation outside the EU are relatively limited. However, there are third party administrative arrangements with countries like Norway, Switzerland and Serbia for example. Beyond this, the primary point of contact with third parties is conducted through the European External Action Service (EEAS), which has so far established several strategic partners. It is not limited to strategic partners though and examples of dialogues that have been established include some on cyber defence and others on cybersecurity and the civil domain with the U.S., China, India and Japan.

The discussion then focused on the regulating or controlling of dual-use technology within Europe. A speaker posited that this must be considered with caveats because the EU's mandate is for defensive capabilities only so it is not applicable to offensive capabilities. In terms of exporting attack capabilities, there will be a European context whereas there will be no or minimum export restrictions for defence capabilities on the civil market. A speaker was then asked about a holistic approach that includes aspects of both cybercrime and cyber warfare. He explained that in order to tackle asymmetric actors, it is imperative to take a wider approach which could be used by both the network and information security community and the law enforcement community. Further, while there are differences in competencies and skills, there is potential for synergy between different stakeholders and communities. In terms of advice for small states such as Singapore if they want to be effective partners in influencing cyber policy in their respective regions, it was suggested that it is important to have further collaboration on cyber defence and cybersecurity issues with organisations from other regions. However, a speaker added that while sharing ideas and solutions is always helpful, states should be able to properly assess whether a framework is suitable for them.

A participant asked whether it is becoming difficult to trace cyber attacks given the increasing sophistication of cyber criminals and the techniques used. A speaker explained that it is not difficult to trace an attack but it is difficult to attribute the act to a person. A speaker was asked about the most critical barriers to international cooperation for law enforcement. Misunderstanding was highlighted as a crucial barrier, which INTERPOL tries to bridge by improving understanding between countries. INTERPOL also faces a challenge in dealing with 21st century crimes by relying on 20th century laws. In an increasingly borderless, "cybered" world, crimes are taking place fluidly across multiple borders. INTERPOL's Cyber Fusion Centre was established to meet the needs of tackling crime in the digital age in order to circumvent the problems presented by traditional diplomatic channels and provide stakeholders with ways to exchange information.

Participants then considered current and future trends. An upward trend in terms of malware was highlighted. For the past year, it seems that the number of attacks has decreased while the number of campaigns has increased. The nature of attacks seems to be more focused and targeted specifically to certain individuals. There are also a lot of opportunities for attackers to leverage, which was not the case previously. For example, current mobile devices are like mini computers and can run programs. There has not been significant attack on mobile phones, but there has been malicious applications stealing information and trying to use that to make expensive phone calls or send out hate messages. Security, however, tends to be sacrificed at the expense of convenience, providing opportunities for attacks.

The discussion considered whether start-ups will spend money on security and a speaker agreed that they do not have incentive to do so at the moment. However, he explained that breaches can be costly, a company may have to close down as a result, and reputation could be affected. Education and awareness is therefore important to increase awareness of security issues for security start-ups. A speaker was then asked about working with governments and whether there are limits on the amount of information that can be shared. He described that it would depend on the relationship between the company and government. A long-term working relationship is more likely to be beneficial in terms of information that could be provided.

Contributed by Yeap Su Yin

DISCUSSION

THE GLOBAL IMPLICATIONS OF THE U.S.-CHINA CYBER RELATIONSHIP

China's Perspective

Zhu Qichao, Director and Professor, Centre for National Security and Strategic Studies (CNSSS), National University of Defense Technology (NUDT), China

Zhu Qichao

Zhu Qichao's presentation outlined the history and challenges of China-U.S. cooperation on cybersecurity. He posited that there is currently limited communications and cooperation on cybersecurity issues that may help to ease the tensions and facilitate strategic mutual trust between the two powers. He concluded by providing suggestions for the promotion of a new type of relations between the major powers.

Zhu noted that since 2010, with the rapid development of China's comprehensive power and continuous expansion of its national interests in cyberspace, cybersecurity has become one of the most important issues impacting on its relationship with the United States. The fear of U.S.-China confrontation over cyber issues like cyber freedom, cyber sovereignty, hacking attacks, intellectual property espionage, and the code of conduct in cyberspace has become a matter of international concern. From the 5 June 2013 disclosure by Edward Snowden of NSA's surveillance programme to the U.S. Department of Justice's prosecution of five Chinese nationals for cyber espionage, no issue has emerged of such importance and generated such level of friction. Zhu highlighted four points of contention between the position of China and the U.S. on cyberspace: (1) respect for sovereignty and freedom in cyberspace. While the U.S. believes that basic freedom in cyberspace should be protected, some countries believe that the U.S. has tended to take advantage of cyber diplomacy and cyber smart power to intervene or even try to overturn governance for its own end; (2) hacking as an international public nuisance that affects both the U.S. and China; (3) current U.S. dominance in Internet governance; and (4) cyber arms control and the international code of conduct.

To reduce confrontation, Zhu observed that the two powers have conducted many forms of cybersecurity communication and cooperation on both the governmental and non-governmental levels since 2009. At the non-governmental levels, Sino-American academics have converged on cybersecurity issues and Track 2 dialogues have been organised on cyber-related issues. Both China and the U.S. have also conducted effective cooperation in terms of joint law enforcement. For example in 2011, police from both sides jointly destroyed the biggest Chinese pornography website in the world.

In addition to establishing cyber relations with the U.S., China has also been active in bilateral and multilateral dialogue in relation to cybersecurity matters with other countries such as the U.K., South Korea, ASEAN countries, the EU, and the African Union. For example, China and the ASEAN members co-sponsored the Cyberspace Forum in September 2014, which is an important part of China's One Belt and Internet Plus initiative. He surmised that this One Belt initiative will make China the backbone of the global Internet district both in terms of the use of numbers and the market values of digital economy.

Zhu stated that, despite the numerous initiatives, positive cyber cooperation between the U.S. and China still faces barriers. Apart from long-standing structural challenges like economic treaties, and the position on Taiwan, four areas pose challenges to U.S.-China cooperation: (1) the U.S. pivot to Asia has increased pressure on

China's national security concerns and cast a lingering shadow on future cooperation for cybersecurity issues; (2) lingering doubt over the United States' willingness to accept China's rise as a global power; (3) whether the U.S. is willing to exercise self-restraint in the cyber arms race and the impact of the U.S. promotion of arms' race in Asia; (4) cognitive differences on cybersecurity issues, especially pertaining to an information technological edge. The U.S. is unrivalled in terms of its IT global technological advantage, contributing to the sense of technological inferiority.

Zhu then noted that although China had suspended the U.S.-China working group on account of the indictment of the five PLA officers, the interdependencies between the two governments are deepening as evident from the restarting of cyber communication during the Strategic and Economic Dialogue this year.

In recommending the way forward, Zhu stated that true bilateral cooperation between the U.S. and China will be difficult to achieve if significant differences between the two powers in terms of strategic decision-making capabilities, IT capabilities, and cyber defence capabilities continue.

Contributed by Jennifer Yang Hui

The U.S. Perspective

Jason Healey, Senior Research Scholar, Arnold A. Saltzman Institute of War and Peace Studies

Jason Healey

Jason Healey's presentation outlined similarities and differences between the U.S. position on cybersecurity with China. He outlined a number of flashpoints in the U.S.-China relationship relating to cyber. In addition, long-term implications of economic or industrial espionage on the international intellectual property rights regime and the digital economy was raised in the course of his speech.

Healey stated that he has found that the overall sentiment in the U.S. and China cyber relationship is one of strategic vulnerability. As the parent of the Internet, the U.S. advocates an open and free Internet. As the sole superpower for the past 20 years, it is also perceived by other countries like China to be dominant in terms of military and intelligence superiority online. Further, the U.S. position and strategic advantages online often clash with China's vision. Whereas the inability to prevent China's commercial espionage to protect national innovation has contributed to the United States' sense of strategic vulnerability. In recent years, however, Healey noted that there have been efforts to overcome mutual suspicion on the United States' side by being more transparent about its cyber operations.

Healey outlined several specific flashpoints in the U.S.-China cyber relationship as including: (1) cross-border content; (2) espionage. He noted that while espionage is an issue that affects both the U.S. and China, there has not been a good norm with regards to spying. Nationalist emotions have also ran high for both powers in the wake of the discoveries of various espionage cases; (3) territorial disputes such as that over the East China Sea, South China Sea, Taiwan issues and Tibet tend to have a spill-over effect for cyber; (4) misunderstanding between both sides. However, he observed that there have been more bilateral dialogues to reduce miscommunication compared to five years ago. While potential for escalation still exists, the situation has improved relative to the late 90s and early 2000s; and (5) North Korea represents a good area for cooperation for both powers, especially after the Sony hacking incident.

In presenting the way forward, Healey noted that the long-term cost of espionage will outweigh any benefit it may offer. He pointed out that there are various common concerns and areas where both sides can cooperate on cyber-related issues. For instance, the East West Institute has a bilateral collaboration on eradicating spam. Healey

also stated that restraint must be exercised on both sides. The U.S., for example, should exercise restraint in monitoring espionage in order to be seen as less aggressive. Finally, he believed that transparency will greatly aid U.S.-China cyber-relations. Including China in both formal and informal trust networks should be an area for future consideration.

Contributed by Jennifer Yang Hui

Discussion

The discussants were asked about the sense of strategic vulnerability that the U.S. and China feel toward each other. A discussant responded that the U.S. attitude towards espionage is multi-layered. On one hand, the superpower itself is extremely competent in the game of espionage. However, its main objective for espionage is to provide military secrets for the government, not for commercial purposes. On the other, China's size and economic power has troubled the U.S. immensely. Commercial espionage hits the U.S. where it hurts most: innovation, where it has based its superpower status for the past few decades. The second discussant noted that the existence of commercial espionage for the sake of aiding rapid growth of development is inevitable. However, the fallout resulting from arresting the individuals suspected for espionage is at times greater than warranted. Chinese officials are therefore understandably upset by the United States' accusation of espionage.

A participant observed that there is a fundamental philosophical difference between how China and the U.S. understand the notion of cybersecurity and construction of the challenges faced, and therefore wondered how this issue will be resolved in future. A discussant stated that China is open to, and has in fact, been active in carrying out bilateral cooperation with other countries. Cyberspace provides both opportunities and challenges for China. On one hand, the increasing number of users means increasing commercial opportunities for China. Premier Li Keqiang has also called for more vigorous innovation online. However, the growth of digital economy means that China will face increasing threats from cyber criminals. The Chinese government has therefore shown great concern about finding ways to enforce the law in cyber-related crimes. China must also deal with IP rights protection in the near future - if a country is unable to establish a foundation of indigenous innovation, growth cannot take place. He also noted that threats from cybercrime will continue in an era where the digital economy is the key to growth.

The other discussant was pessimistic about the resolution of the differences. Espionage is likely to continue due to the strategic vulnerability that both feel towards each other. Both also take opposing stands with regards to the freedom and flow of information across borders. The U.S. believes that there should be a free flow of information across its borders, as stipulated by its Constitution. China, on the other hand, sees the free flow of information as being dangerous to its regime.

The session concluded with a discussion on the global implications of the U.S.-China cyber relationship. A discussant stated that the U.S. and the world should adopt a more positive attitude towards an increasingly confident China in both cyber and non-cyber-related issues. For other countries, such as Singapore, there are many opportunities for involvement in cyber-relevant issues. On the strategic level, Singapore, for example, may create new platforms for cooperation on cyber-related dialogues. At a practical level, Singapore could also develop cooperation with countries like China in areas where it is seen as a model (such as industrial modernisation and the building of smart cities). The other discussant concluded that power play will continue to dictate cyber norms instead of law.

Contributed by Jennifer Yang Hui

Panel 5:

EMERGING TECHNOLOGY TRENDS AND THREATS

Possible Challenges to International Humanitarian Law: Lethal Autonomous Systems and Cyber Implications

William H. Boothby, Associate Fellow, Geneva Centre for Security Policy

William H. Boothby emphasised the diversity of unmanned weapons and highlighted the distinction between man-in-the loop and man-on-the loop systems. The former is based on an individual's decision to comply with targeting laws, to evaluate proportionality and to initiate or abort a planned attack. By contrast, the latter refers to a system that may be capable to make its own attack decisions.

While automation was defined as a response to sensor inputs and acts, an autonomous system is aware of its environment and able to make high-level decisions, including the independent identification of one or several target(s). Reviewing different articles of the 1977 Additional Protocol I to the Geneva Convention of 1949, Boothby listed the major legal debates related to autonomy. Some of these contentious issues regard the (non)distinction made by the machine between different categories of individuals such as combatants, non-combatants, civilians and hors-de-combat; the possible decision to minimise civilian dangers ; and the level of assessment of military advantage as well as risks posed to civilians. Nevertheless, potential benefits of autonomous systems include the alleged removal of human error and a possibly more cautious approach to the decision-making process related to the launching of armed attacks.

Boothby noted that autonomous technology is a long way off according to some and, while he has doubts about the maturity of such technology, there are clearly legal difficulties.

In terms of cyber, he noted that many points he raised regarding autonomy apply to cyber. Further, while it might sound good, the separating of military and civilian infrastructure is questionable, especially with satellite systems.

From a cyber perspective, key issues relate to the definitions of a cyber attack or computer network attack (CNA) and a cyber weapon. Serious and dramatic consequences of malicious cyber activities make it possible to characterise a CNA. These include material damage; loss of functionality requiring the replacement of physical components; injuries and death of individuals. By contrast, a cyber weapon refers to any cyber capability used, intended, or designed to cause injury or damage.

Boothby agreed, in concordance with the authors of the Tallinn manual, that the jus in bello applies in cyberspace. He explained that by making legal sense of the notion of cyber attack, the Tallinn experts were able to apply much of the law of targeting, in both customary law and in articles 48 to 67 of Additional Protocol I to cyber operations that amount to cyber attacks, as that notion is defined in the Manual.

Similarly, the legal identification of a cyber weapon allowed these experts to apply the law of weaponry rules to cyber facilities coming within the definition of cyber weapon. Therefore, he inferred that elements of the jus in bello that are related to these two categories of laws apply to the wider field of cyber operations and cyber capabilities. As the critical role of IT to targeting is likely to grow exponentially, Boothby emphasised the need for robust cyber systems. He showed skepticism on the prospect of a new customary rule and treaty law but expressed, nevertheless, his belief in the narrowing of differences between Western and Russian/Chinese perceptions of cyberspace.

Contributed by Romain Brian Quivooij

Q&A Session

A participant enquired if the law should be expected to lead future discussions as well as how principles should be formulated, or if the law would be reduced to being responsive to strategic realities of what nation states are actually doing. Boothby opted for the second alternative which, as he stated, increasingly applies to

the fields of autonomous weapons systems and cyber warfare as well as other domains.

However, basing his analysis on the content of customary law, he added that evolving state practice had a significant impact in the development of the law. Boothby expressed doubts as to the idea that these legal developments would be carried out at a similar pace between different areas of evolving weapons technology. As an example, he mentioned the field of synthetic biology to illustrate some limitations brought to research, the 1972 biological weapons convention in this particular case.

Contributed by Romain Brian Quivooij

The Cybersecurity Landscape in India
Rahul Sharma, Senior Consultant, Data Security Council of India

Rahul Sharma

Rahul Sharma discussed some of the major programs and initiatives launched by the Data Security Council of India (DSCI), an industry body for data protection set up by the National Association of Software and Services Companies (NASSCOM).

Among the range of national security concerns related to cybersecurity, Sharma mentioned the significant threat of ICT supply chain risks; the development of offensive cyber capabilities by military intelligence agencies as well as the lack of information-sharing and global cooperation. Faced with such challenges, countries have to develop strategies to keep themselves relevant in the cyber domain. He further noted that industry opposes data localisation as it believes that this is counter-productive in the long run, even where it might assuage short term concerns.

Citing further problems associated with Internet governance and privacy, Sharma explained that while a few countries have a strategic advantage in the management of the Internet, the control of critical Internet resources is central. Likewise, privacy-related matters have become ever more important as today's cyber threat landscape encompasses a wide spectrum of malicious activities ranging from cybercrimes to attacks on critical infrastructure and cyber espionage. In response, India has set up a dense network of government departments and agencies, including structures attached to the Ministry of External Affairs, the Ministry of Defence, and the Ministry of Commerce. This wide ecosystem is now overseen by a cybersecurity coordinator.

To understand the range of existing cybersecurity initiatives in India, it is necessary to distinguish between policy initiatives and guidelines; regulatory frameworks and institutional mechanisms. The former involves a series of national measures launched between 2012 and 2015, including the 2013 National Cyber Security Policy. In terms of regulation, Sharma emphasised the importance of the Information Technology Act which covers many aspects of the cyber domain. Varied bodies such as the Reserve Bank of India and the Insurance Regulatory and Development Authority (IRDA) contribute to the issuance of regulatory guidelines. The establishment of joint working groups within the framework of PPPs was mentioned as a fruitful initiative. Such institutional mechanisms place a strong focus on data protection, capacity building, information-sharing, and awareness.

Shifting to privacy-related issues and challenges, Sharma underlined the variety of perspectives involved. In setting up initiatives that have implications on privacy, the Indian government is faced with the crucial need to balance privacy concerns with the imperatives of national security requirements and business growth. The lack of a comprehensive privacy law in India adds to the complexity of a fragmented domain where private companies have their own priorities.

To conclude, Sharma commented on some of the major

declarations related to Internet governance made by the BRICS association, and tackled the key issue of the international jurisdiction of ICANN. The IANA transition is appreciated and he noted that India upholds the multi-stakeholder model of Internet governance, although the latter still needs to be defined.

Contributed by Romain Brian Quivooij

Arms Control Issues relating to Cyber

Sean Kanuck, National Intelligence Officer for Cyber Issues, National Intelligence Council, Office of the Director of National Intelligence

Sean Kanuck

Sean Kanuck announced the launch of an international effort by the National Intelligence Council to better frame the analytical discussion on arms control in cyberspace. An implicit question is to know whether arms control is desirable or even feasible.

Kanuck characterised the cyber domain as inherently insecure and volatile. He outlined a picture of the cybersecurity environment, as drawn by the Director of National Intelligence in 2015. Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyber attacks, due to the absence of universally accepted and enforceable norms of behaviour in cyberspace. The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. This leads to a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve and thresholds. Additionally, the muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation.

Kanuck then explained the National Intelligence Council's analytical views on four widely discussed topics. First, cyberspace is not a "global commons", as all ICT nodes are subject to proprietary interests and sovereign jurisdiction. Second, cyberspace is not a separate and unique "domain" for conflict, as cyber operations occur (and their effects are manifested) on land, at sea, in the air, or in outer space. Third, not all malicious cyber activities constitute attacks, which refer to disruptive and destructive activities. Fourth, a "cyber armageddon" is an unlikely scenario, but low-to-moderate level cyber attacks are already causing cumulative harm to economic competitiveness and national security.

Proposed limitations on cyber activities rely on norms of behaviour for state actors, confidence building measures (CBMs) and international humanitarian law.

Kanuck then outlined a conceptual framework. The notions of second and third-party deterrence, disarmament and arms control were respectively defined as limitation to actions; actors and capabilities; effects.

First, he outlined four required elements for cybersecurity architecture. He suggested four minimum standards: 1) he underlined the central need for transparency, as rules and limitations need to be clearly and publicly articulated. Documents should be made public and they should be shared, otherwise other parties will not know your intentions. For example, the exchange of military white papers; 2) cybersecurity architecture should be universal, without being symmetric; 3) enforceability is critical, because credibility is based on the ability to detect, monitor and verify. However, the latter is an incredibly challenging task, as countries are reluctant to disclose information related to the nature of their cyber activities; 4) stability should be the cornerstone of this system, to the point of establishing and maintaining a Nash equilibrium. The latter refers to a situation where two or more players know the equilibrium strategy of each other and will not modify their own strategies, due to the lack of gain that would result from such changes (Countries are still figuring out their strategies).

Kanuck then outlined nine sources of cyber insecurity and instability. He mentioned the dualistic, non-severable, and multi-polar dimensions of the cyber environment. As instruments of cyber surveillance are used to deliver offensive capabilities, he characterised the cyber environment as dualistic. Different situations such as conflicts like the "Arab Spring" and Crimean crisis are merged with cyberspace, which makes it a non-severable domain. Further, it is multi-polar, as many non-state entities can play a significant role.

He further explained that cyber tools are perishable. Once they are used, malwares are identified, analysed and possibly re-used by the victim(s). Additionally, a cyber weapon is specific because it must be designed for a given victim network. Immediacy is a third distinctive feature as ready-to-use capabilities are necessary to survive an adversary's first strike.

Kanuck concluded by underlining the clandestine nature of cyber operations, given that nation states do not take credit for cyber attacks they initiate. Further, cyber operations should be considered indiscriminate, as they target civilian and military networks. Unpredictability remains strong, due to the uncertainty surrounding the exact impact of cyber operations and the fulfillment of objectives it is designed to achieve.

Contributed by Romain Brian Quivooij

Discussion

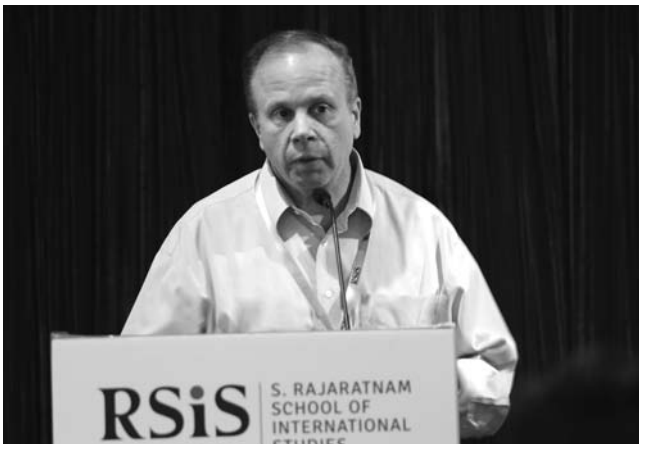
A participant asked about cross-domain deterrence. A speaker stated that the United States, China, and Russia reserve the right to respond, either through one domain or a cross-domain approach, if they feel certain that thresholds have been crossed in cyberspace. He added that most nations look at the response options to include cross-domain capabilities. However, no country was said to have any firm decision on exactly how it would respond if it would face a genuine critical cyber attack. To illustrate his point, he recalled that the U.S. decided to respond with economic sanctions against North Korea, following the cyber aggression directed against Sony Pictures Entertainment. Another participant asked about uncertainty between states and the nature of their respective cyber capabilities. A speaker agreed that legal and technical uncertainty substantially increases insecurity. He emphasised the crucial need for clear and publicly articulated rules so that everyone knows how they are expected to behave in cyberspace.

Contributed by Romain Brian Quivooij

CLOSING ADDRESS

Technology, Threats and Trust in an Interconnected World

Robert Butler, Managing Director, Cyber Strategies LLC



Robert Butler

Robert Butler discussed the interrelated components of technology, threats, and trust and how these can provide a robust future for cybersecurity stakeholders. For technology, Butler explained that the Internet of Things (IoT) paved the way for smart technologies that were unheard of only a few years ago. The defining characteristics of IoT and the convergence of operational and information technology have a bright potential in terms of reach and scale. Butler stressed that moving forward, IoT key enablers such as affordable bandwidth and processing, smartphones, wireless coverage, cryptography, and big data are going to be interconnected with each other and to people's day-to-day ways of living. He added that partnerships between business and technology are also developing immensely as advancements in IoT continue to accelerate in an exponential way. However, he pointed out that when we think about technological capabilities and efficiency, the subject of threat or risks is inevitable.

With regard to threats and vulnerabilities in the industrialised Internet, Butler highlighted that there have been many surveys but one most recently by HP shows that relating to program logic controllers, industrialised DCSs and Scada systems, on average, in a sample of any kind of particular industrial control system set, approximately 70 per cent of the devices show obvious vulnerabilities. While innovation is moving at a phenomenal pace, risk exposure is therefore much greater than what has been seen in the past. He further argued that the exploitation of privacy in smart devices is becoming more pervasive. He added that it is important to think about the future of indirect access as there have been a number of recent attacks and breaches in service and sales systems which affected thousands of people.

Butler explained that as we move to a technological age of smart devices, we face a new set of risks which are not only privacy-related but also safety related, thus we should look at threat actors. Adversaries are looking at vulnerabilities as exploitation vectors to disrupt, degrade, and destroy. He described that threat actors range across a variety of categories and we are now in a situation where we can see asymmetrical capabilities being used against critical infrastructure, intellectual property, and security of nation states and transnational actors.

He posited that we are now in the age of the three Cs—people are either going to Cooperate, Compete, or Conflict. Since there is an unequal distribution of resources, we need to strive for cooperation and competition as opposed to conflict. We are building a global interconnected transaction platform, and communities, regions, and nations are dependent upon it. We need speed and agility to be able to move across regions and communities especially when things go bad;,to be able to understand how to rapidly take resilient structures and use them in appropriate ways; to shift workloads; and to remedy issues as they arise.

After discussing the complexities of technology and threats, Butler then argued it is necessary to create a framework of trust so that partnerships and collaborations could be successfully put into action. He pointed out that there is a need to come together and start building models of trust with norms and principles that extend across governments, societies, businesses, and academia.

Butler enumerated three models of trust exhibiting proactive collaboration. First, he discussed the Japanese/JP cert as a model of collaboration that

works on incident response as it not only scales across Tokyo and the rest of Japan in terms of national response but also across the region as it functions as the executive secretariat for the AP-CERT. Second, he highlighted Singapore's hosting of INTERPOL's Global Complex for Innovation as a model for proactively bringing nations and industries together in campaigns. He mentioned the recent botnet takedown campaigns where law enforcement from different countries worked with industry and took proactive action to clean up cyberspace. Third, he discussed the Financial Services Information Sharing and Analysis Center (FS-ISAC) where financial institutions work together as it extends globally.

He explained that the ingredients for successful partnerships are the identification of champions, experts, and top performers; strong group commitment to common goals and objectives; adoption of shared operating principles and standards; and focus on delivering enduring value and best practices.

Contributed by Priscilla Cabuyao

DISCUSSION ON KEY TAKEAWAYS

Sean Kanuck, National Intelligence Officer for Cyber Issues, National Intelligence Council, Office of the Director of National Intelligence

Sean Kanuck first underscored the rise of high-level policy attention and international focus on cybersecurity as well as the technical and policy threats that range from matters like Internet governance to the destabilising nature of certain information flows to sovereignty issues.

Kanuck underlined the importance of discussing cybersecurity in the context of international relations theory and dealing with strategic concerns as well as ways to better cooperate and overcome the challenges of attribution, verification, and uncertainty. He shared that the points relating to CBMs, proxy actor concerns, and battling cybercrime in the ASEAN and Asia Pacific region were significant. He also found that the segment on the Sony Entertainment Pictures attack raised critical questions and lessons for future actions regarding cyber attacks given the potential impact on national interest and society.

The discussion on the rights of citizens vis-à-vis security concerns illuminated how citizens could protect themselves through technology as well as the importance of finding the right "balance". Kanuck then pointed out that the discussion on developments and frameworks in cybersecurity provided lessons on the trade-offs between national security and criminal law as well as the state's rights when it comes to civil liberties. He further stressed the impact of national security on creativity and innovation. He observed the qualified nature of freedom of speech in every country and the fact that at some point, there is certain limitation. However, the question to then consider is where this line should be drawn. In particular, significant questions include: 1) who guards the guardians; 2) who places limits on limits; 3) do human rights place limits on sovereign governments; and 4) do governments place limits on how one can exercise human rights within cyberspace?

Kanuck noted the multiplicity of countries acknowledging their offensive capabilities and added that this initial degree of transparency is a small step in the right direction in terms of stakeholders' discussions on security. He emphasised the points made relating to dependence on energy and telecommunications, and how these sectors are civilian resources which will be military targets if there were a military cyber conflict. He was concerned about how they could possibly be legitimate targets under Hague law.

Kanuck then questioned whether national security implications should always trump economic security when policies are being formed. He further considered the role of the private sector, particularly security companies, in terms of helping to defend networks as well as assess and attribute cyber intrusions. He underscored that intelligence analysis on cyber intrusions is no longer the purview of governments. He described this shift toward working with the private sector as monumental and one of the three biggest trends he has noticed. Private sector security companies have tremendous information sources and an ability to assimilate information. They are therefore in a position to collaborate with each other and with government as appropriate. He argued that early warning as well as testing of the security and resilience of networks is essential.

In terms of the exchange on the U.S.–China relationship, he underlined that such discussions in an international workshop are important. He observed that despite the incredible economic interdependence between the two countries and many views they share in common, they do not have the same perfectly assimilated policy views. However, sharing these thoughts in an environment like the CENS cybersecurity workshop is beneficial. He considered that this exchange of opinions in an international workshop helps serve as a CBM in itself and it will possibly help find collective norms.

He raised the points that were made regarding ethics and whether it is in fact irresponsible to produce applications without security features. In terms of smart nations and IoT, Kanuck raised their undeniably significant role in the future. Future concerns of both the public and private sectors will undoubtedly be driven by the advancements in IoT and smart nations.

However, he noted that while such developments come with risks, they could be managed through confidence and trust.

Robert Butler then stressed the importance of actionable steps and he called for more actions to be taken in order to achieve goals so that there is a move from dialogue to tabletops and action-oriented steps.

Caitríona Heinl enumerated some key observations from discussions held at the workshop. She noted: 1) the developments in the region in terms of CBMs and the significance of the work of the ARF and OSCE; 2) the importance of international human rights even where there are cultural differences; 3) the increasingly important implications concerning the inseparability of civilian and military infrastructures; 4) clarifying how international law below the level of armed conflict applies; 5) the need for more discussions, increased transparency, and real action points; 6) the importance of considering how to spur innovation while ensuring security measures are in place; 7) the link between the cyber and energy sectors as well as smart nation initiatives. Moreover, the need to incorporate security and privacy in all smart city projects; 8) how to avoid market barriers and encourage a global market for ICT when addressing national security; 9) the importance of cyber arms control; 10) how Singapore could play a role in facilitating cooperation in the region; 11) the necessity to deal with the legal difficulties relating to increasingly autonomous technologies; 12) the call for increasing transparency, publicly shared documents and the exchange of white papers; and 13) the need to build models for trust.

Tobias Feakin emphasised that the findings of these workshops make a difference. Wouter Jurgens acknowledged the rich discussion that the workshop provided and how useful it is to exchange views with participants from public and private sectors, academia, and civil society. He explained that having discussions between representatives from various continents is part of a bigger process and strategy that is crucial for the future. By continuing such discussions in this way, it will assist when facing dilemmas and formulating international cyber strategies, policies, and doctrines.

Contributed by Priscilla Cabuyao

WORKSHOP AGENDA

Monday, 20 July 2015

0800 – 0830hrs **Registration**

0830 – 0845hrs **RSIS Corporate Video & Welcome Remarks by Shashi Jayakumar,** *Head, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), NTU*

0845 – 0900hrs **Opening Address** *by* **Ambassador Ong Keng Yong,** *Executive Deputy Chairman, S. Rajaratnam School of International Studies (RSIS), NTU*

0900 – 0945hrs **Keynote Address** *on* **"Cyber Foreign Policy: Threats and Opportunities"** *by* **Christopher M.E. Painter,** *Coordinator for Cyber Issues, Office of The Secretary, U.S. Department of State*

Chairperson :
Shashi Jayakumar, *Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Q & A

0945 – 1000hrs **Tea Break**

1000 – 1100hrs **Panel 1: Cyber and International Security: Opportunities and Challenges for Further Cooperation**

Chairperson :
Shashi Jayakumar, *Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers :
"Broadening Debates on International Peace and Security in Cyber" *by Wouter Jurgens, Head of International Cyber Policies, Security Policy Department, Ministry of Foreign Affairs, The Netherlands*

"Confidence Building Measures at Regional Level: What is New and on the Horizon" *by* **Yono Reksoprodjo,** *Expert Staff, National Desk for Information Resilience & Cyber Security, Coordinating Ministry for Politics, Legal & Security Affairs, Republic of Indonesia*

*"***Redlines in Cyberspace – What the Sony Attack means for State Responses to Cyber Incidents"** *by* **Tobias Feakin,** *Senior Analyst and Director, International Cyber Policy Centre, Australian Strategic Policy Institute*

1100 – 1215hrs **Syndicate Discussions**

Syndicate 1
Venue :
Vanda Ballroom, Level 5

Syndicate 2
Venue :
Vanda 5, Level 6

Syndicate 3
Venue :
Vanda 6, Level 6

1215 – 1315hrs **Lunch**
Venue :
Pool Garden, Level 5

1315 – 1445hrs **Panel 2: Squaring National Security and Data Privacy Matters**

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

Speakers :
"Managing Data Privacy and Civil Liberties Activities" *by* **Simon Chesterman,** *Dean, Faculty of Law, National University of Singapore*

"Cybersecurity and the Balancing of National Security with Data Privacy and Freedom of Expression - the Philippines Perspective" *by* **Geronimo L Sy,** *Assistant Secretary, Department of Justice, The Philippines*

"Balancing National Security Needs with Data Privacy and Freedom of Expression Concerns: Singapore's Perspective" *by* **Bryan Tan,** *Partner, Pinsent Masons MPillay LLP, Singapore*

Q & A

1445 – 1500hrs **Tea Break**

1500 – 1600hrs **Panel 3: Digital Economy**

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

Speakers :
"Public-Private Partnerships from an Industry Perspective" *by* **Jan Neutze,** *Director of Cybersecurity Policy, Microsoft EMEA*

"Securing and Optimising the Next Wave of Innovation in Smart Cities" by Michael Mylrea, *Chief Information Security Officer, Cyber Innovation Development*

"The Economic Security Implications of Cybersecurity" *by* **Daniel Castro,** *Vice President, Information Technology & Innovation Foundation*

1600 – 1700hrs **Syndicate Discussions**
Syndicate 1
Venue :
Vanda Ballroom, Level 5

Syndicate 2
Venue :
Vanda 5, Level 6

Syndicate 3
Venue :
Vanda 6, Level 6

1700hrs **End of Day 1**

1800 – 2030hrs **Workshop Dinner (by invitation only)**
Venue :
Lotus Room, Peach Blossom, Level 5

Tuesday, 21 July 2015

0800 – 0830hrs **Registration**

0830 – 0915hrs **Keynote Address** *on* **"Cybersecurity Trends and Issues from a Singapore Perspective"** *by* **John Yong,** *Director, Infocomm Security Group, Infocomm Development Authority of Singapore.*

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

Q & A

0915 – 0930hrs **Tea Break**

0930 – 1030hrs **Panel 4: Cyber in Practice – Key Developments**

Chairperson :
Michael Raska, *Research Fellow, RSIS, NTU*

Speakers :
"The Fight against Cybercrime and Cybersecurity: How to Converge in a More Efficient Way?" *by* **Christophe Durand,** *Head of Cyber Strategy, Strategy & Outreach, Cyber Innovation and Outreach Directorate, INTERPOL Global Complex for Innovation &* **Steve Honiss,** *National Cyber Review Manager*

"The Strategic Approach of the EU to Cybersecurity and Defence" *by* **Wolfgang Roehrig,** *Programme Manager & Project Officer, Cyber Defence, European Defence Agency*

"Intelligence Gathering and Analysis in Cyberspace" *by* **Eugene Teo,** *Senior Manager, Symantec Security Response, Symantec Asia Pacific*

1030 – 1145hrs **Syndicate Discussions**

Syndicate 1
Venue :
Vanda Ballroom, Level 5

Syndicate 2
Venue :
Vanda 5, Level 6

Syndicate 3
Venue :
Vanda 6, Level 6

1145 – 1300hrs **Lunch**
Venue :
Pool Garden, Level 5

1300 – 1400hrs *Discussion:*
The Global Implications of the U.S. – China Cyber Relationship
Moderator :
Teymoor Nabili, *Executive Editor, Channel NewsAsia*

Speakers :
"The U.S. Perspective" *by* **Jason Healey,** *Senior Research Scholar, Arnold A. Saltzman Institute of War and Peace Studies*

"China's Perspective" *by* **Dr Zhu Qichao,** *Director and Associate Professor, Centre for National Security and Strategic Studies (CNSSS), National University of Defense Technology (NUDT), China*

Q & A

1400 – 1415hrs **Tea Break**

1415 – 1545hrs **Panel 5: Emerging Technology Trends and Threats**

Chairperson :
Norman Vasu, *Deputy Head, CENS, RSIS, NTU*

Speakers :
[SKYPE] "Possible Challenges to International Humanitarian Law: Lethal Autonomous Systems and Cyber Implications" *by* **William Boothby,** *Associate Fellow, Geneva Centre for Security Policy*

"The Cybersecurity Landscape in India" *by* **Rahul Sharma,** *Senior Consultant, Data Security Council of India*

"Arms Control Issues relating to Cyber" *by* **Seán Kanuck,** *National Intelligence Officer for Cyber Issues, National Intelligence Council, Office of the Director of National Intelligence*

Q & A

1545 – 1600hrs **Tea Break**

1600 – 1645hrs **Closing Address on "Technology, Threats and Trust in an Interconnected World"** *by* **Robert Butler,** *Managing Director, Cyber Strategies LLC*

1645 – 1700hrs **Moderated Discussion on Key Takeaways**

Moderator :
Seán Kanuck, *National Intelligence Officer for Cyber Issues, National Intelligence Council, Office of the Director of National Intelligence*

1700hrs **End of Day 2**

1800 – 2030hrs **Closing Dinner (by invitation only)**
Venue :
Aquamarine, Level 4

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

William Boothby
Associate Fellow
Geneva Centre for Security Policy

Robert Butler
Managing Director
Cyber Strategies LLC

Daniel Castro
Vice President
Information Technology and Innovation Foundation

Simon Chesterman
Dean
Faculty of Law
National University of Singapore

Christophe Durand
Head of Cyber Strategy
Strategy & Outreach
Cyber Innovation and Outreach Directorate
INTERPOL Global Complex for Innovation

Tobias Feakin
Senior Analyst and Director
International Cyber Policy Centre
Australian Strategic Policy Institute

Jason Healey
Senior Research Scholar
Arnold A. Saltzman Institute of War and Peace Studies

Steve Honiss
National Cyber Review Manager
INTERPOL Global Complex for Innovation

Wouter Jurgens
Head of International Cyber Policies
Security Policy Department
Ministry of Foreign Affairs
The Netherlands

Seán Kanuck
National Intelligence Officer for Cyber Issues
National Intelligence Council
Officer of the Director of National Intelligence

Michael Mylrea
Chief Information Security Officer
Cyber Innovation Development

Jan Neutze
Director
Cybersecurity Policy
Microsoft EMEA

Christopher M.E. Painter
Coordinator for Cyber Issues
Office of The Secretary
U.S. Department of State

Yono Reksoprodjo
Expert Staff
National Desk for Information Resilience & Cyber
Security Coordinating Ministry for Politics, Legal &
Security Affairs Republic of Indonesia

Wolfgang Roehrig
Programme Manager & Project Officer, Cyber Defence
European Defence Agency

Rahul Sharma
Senior Consultant
Data Security Council of India

Geronimo L Sy
Assistant Secretary
Department of Justice
The Philippines

Bryan Tan
Partner
Pinsent Masons MPillay LLP
Singapore

Eugene Teo
Senior Manager
Symantec Security Response
Symantec Asia Pacific

John Yong
Director
Infocomm Security Group
Infocomm Development Authority of Singapore

Zhu Qichao
Director and Professor
Center for National Security and Strategic Studies (CNSSS)
National University of Defense Technology (NUDT)
China

CHAIRPERSONS

Damien D. Cheong
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)

Caitríona H. Heinl
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)

Shashi Jayakumar
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)

Teymoor Nabili
Executive Editor and Presenter
Channel NewsAsia

Michael Raska
Research Fellow
Military Transformation Programme
S. Rajaratnam School of International Studies (RSIS)

Bilveer Singh
Adjunct Senior Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)

Norman Vasu
Senior Fellow and Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)

ABOUT CENS

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.

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://www.nscs.gov.sg/

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