CENS – GFF Cyber-Security Workshop: Towards a Secure and Resilient Cyberspace

12–13 JULY 2010
SINGAPORE

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University
PONDER THE IMPROBABLE

NATIONAL SECURITY COORDINATION SECRETARIAT

GLOBAL FUTURES FORUM
[illegible]

CENS – GFF Cyber-Security Workshop: Towards a Secure and Resilient Cyberspace

12–13 JULY 2010
MARINA MANDARIN HOTEL
SINGAPORE

REPORT ON THE WORKSHOP JOINTLY ORGANIZED BY
THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (SINGAPORE)
AND
THE GLOBAL FUTURES FORUM (INTERNATIONAL)

WITH THE SUPPORT OF
THE NATIONAL SECURITY COORDINATION SECRETARIAT (SINGAPORE)

Contents Page

Rapporteurs: Jenna Park, Clinton Lorimore, Yeap Su Yin, Yolanda Chin and Ng Sue Chia

Edited by: Ng Sue Chia

This report summarizes the proceedings of the conference as interpreted by the assigned rapporteurs and editor of the S. Rajaratnam School of International Studies. Participants neither reviewed nor approved this report.

The conference adheres to a variation of the Chatham House rules. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

Online terrorist communication has driven concerns that violent extremist groups/individuals have advanced from disseminating propaganda on the Web to conducting multi-level outreach activities and possibly planning cyber-based attacks on par with real-life wars. While the threat of cyber-terrorism seems impending, it also highlights a range of potential cyber-threats to national security that needs to be addressed fairly quickly. They range from online financial fraud to the pilferage of personal identities and state information by criminals and state-backed hackers.

Recent Botnets, or Internet Robots, attacks have illustrated the ease at which cyber-attacks can be conducted. A network of computers could be infected and, thereby, setting off a domino chain of database and systems crashes without the need for a highly skilled computer engineer to carry out the attack. The mainstreaming and incorporation of advance communication technologies into such devices as smart phones and game consoles has drastically changed the way information is owned, exchanged and modified. Anyone with a Wifi-enabled phone, for instance, is capable of transmitting information to the cyber-community and altering public perception.

As such, the Centre of Excellence for National Security (CENS), a research unity of the S. Rajaratnam School of International Studies, and the Global Futures Forum (GFF), with the support of the National Security Coordination Secretariat (NSCS), part of the Prime Minister's Office, Singapore, jointly organized a two-day workshop (12–13 July 2010) on "Cyber-Security: Secure and Resilient Cyberspace" to deliberate on ways to counter current and emerging cyber-threats from a whole-of-society approach. The workshop was held at the Marina Mandarin Hotel, Singapore, and was well attended by a multi-disciplinary cast of research analysts, technologists and national security officers.

The workshop commenced with a welcome dinner lecture (11 July 2010) by **Sheila Ronis** where participants of the workshop gained an overview of the challenges to national security. She noted in particular that a synthesized approach that combines foresight tools, hyper-accelerated learning and integrated government decision-making processes are the pre-requisites to the successful countering and anticipation of current and impeding cyber-security threats. Similarly, the need for a whole-of-society approach towards cyber-security was underscored by **Mr. Peter Ho**, Head of the Singapore Civil Service and Permanent Secretary for National Security and Intelligence Coordination, in his welcome address.

The implications that cyber-security breaches have on national security are broad and far-reaching. Indeed, **Ruth David** highlighted that a key challenge to cyber-security is perhaps in the development of counter-attack strategies that would be followed through by governments, corporations and private Web-users alike. Given the dependency on Web-based technologies for daily operations and day-to-day chores, states, corporations and individuals are inevitably affected when a seemingly remote network or database crashes whether as a result of an unintentional technological fault or a deliberate attack.

It is generally agreed that to counter cyber-threats, there needs to be collaboration among all sectors of a society and between states. It may sound Cliché, but, the threat certainly lies in the borderless and virulent nature of cyber-attacks of any sort. As such, cooperation and collaboration are imperatives to outwitting, outlasting and outlawing the perpetrators and malwares per se. Against this backdrop the **Honourable John Grime**s and **John Savage** stressed, over and above other recommendations, the importance of information sharing and international partnerships in moving ahead of our adversaries.

David Auscmith, on the other hand, opined that cyber-defence is only as effective as our existing intelligence or knowledge of the threat allows it to be. Similarly, **Alexander Lim** articulated the Interpol's preference to train law-enforcement personnel to better understand the uses of existing tools over random investments into technologies that may not add to existing intelligence over the current threat scenario. **Anthony Lim** also added that applications cannot be expected to "defend themselves". It was asserted that the best way to prevent an application attack is to ensure that the gap between software design and information security is bridged. Moreover, **Tyson Macaulay** also argued that most anti-virus software is no more than 60 per cent effective at detecting and removing novel pieces of malware. He argued that it is only through information sharing and gathering from multiple sources, that cyber-resilience could be built.

Applications security aside, **Lori Lessner** spoke on violent extremists' presence and their modus operandi in the cyber-sphere. In particular, it was highlighted that violent extremists are switching from the traditional "call to prayer" Web-postings to the creative usage and uploading of rap videos online to appeal to a resentful and "online" youth group. On the same theme, Sarah Womer shared with participants how a closer examination of the "online enemy" and their activities in the cyber-sphere could provide vital indications of impeding real-life plots. In the Philippines' context, **Nicolas Ojeda** argued that a general lack of understanding by key government and private stakeholders over the seriousness and impact of both current and emerging cyber-threats have thus far impeded any improvements in countering, for instance, the Abu Sayyaf Group's communication with the world through new media technologies.

Similarly concerned with cross-sector cooperation and the dual functions of Web-based communication technologies, the finance and telecommunication sectors face a dilemma of securing their networks and making their services as accessible to public usage as possible. **Gunawan Husin** added that the financial sector, being the first line of defence, is under tremendous pressure to counter the possible abuse of online financial services and products for criminal and terrorism purposes. There is also the difficulty in getting financial institutions based in different jurisdictions to conduct regular checks on suspicious financial acts. In India's case, Srijith Nair mentioned that despite the new cyber-security measures in place, a well-thought-out and cohesive cyber-strategy is still lacking. In contrast, **Zahri Yunos** shared that Malaysia has in place a cyber-threat mitigation plan that spells out the roles that its ministries have to take in the guarding of Malaysia's cyber-dependent infrastructures.

Finally, from a policy point of view, **David Edelman** opined that no single lens could give a complete representation of the complexity of cyberspace. He stressed that the goal in the next 10 years in policy circles is to develop and incentivize an international system whereby states see an intrinsic value in a productive and stable cyberspace. **Tyson Macaulay**, however, cautioned that most policies and policymakers do not take into account Critical Infrastructure Interdependency (CII) relationships. A shut down in one component of a critical infrastructure, he emphasized, could bring about major disruptions to systems. As such, Manabu Nabeshima mentioned that the incorporation of CII analysis would not only give policymakers a fuller picture of the impact of a critical infrastructure shutdown but also offer them a range of possible scenarios. As for Japan, existing policies and measures undertaken in the field of information security aims to perpetuate the tradition of public-private sector cooperation. It was argued that as what is being protected belongs to the private sector, Japan's information security policies have been designed to allow room for the society to take appropriate measures to secure their own information networks and systems.

As a final roundup of ideas and suggestions put forth during the discussion panels and syndicate sessions, the workshop closed with a roundtable discussion on the immediate actions to take. It was generally agreed that:

1. A legal framework needs to be established. As current responses to threats tend to be reactive, expertise can be better consolidated when a legal framework is in place;
2. An operational definition of "cyberspace" would reduce conceptual ambiguity and allow for workable solutions to be devised. However, this should not be at the expense of developing high impact solutions;
3. There needs to be a holistic approach towards cyber-security. To this end, three areas for development were identified. The first was the need for robust technology to protect information assets, namely through the development of secure applications. The second was securing the expertise to develop and manage the systems in place which requires equipping staff with the relevant expertise to deal with the various challenges. The third was putting in place clear processes, namely policies, guidelines and standards; and
4. There is no time for consensus. Confidence building should concurrently be complemented with a pragmatic focus on quick wins—the devising of simple policy fixes to address surmountable problems.

All in all, cross-sector collaboration is crucial in a field like cyber-security where transactions cut across jurisdictions and, more often than not, have a domino impact on the way various critical infrastructures are managed and run.

WELCOME DINNER SPEECH
CYBER-SECURITY WITHIN A GLOBAL CONTEXT

Sheila Ronis delivering her Welcome Dinner Speech.

Sheila Ronis gave participants an overview of the cyber-security landscape and highlighted several pressing national security concerns as "food for thought".

The definition of national security has become complex in a world marked by inter-dependency especially in a twenty-first-century environment marked increasingly by inter-connectedness and cross-cutting challenges. Therefore, a wide range of traditional and innovative strategies and tactics have to be considered and applied when countering current-day threats.

In view of the "realities" we are confronted with and the scenarios that could possibly emerge in the future, Ronis made the following observations: (i) The world is a system; (ii) Our homelands are no longer protected by distance or time; and (iii) Globalization demands a holistic world-view.

As global inter-dependence is a reality, Ronis asserted that the world should be thought of as a system where movement or damage in one spot is likely to have a ripple effect on the global community. It was thus opined that cyber-security issues would have a Web-like effect on the global system. Moreover, traditional geopolitical boundaries and time-zones could no longer buffer states from external affairs. National security has, at least for the United States, merged into a "mess" of internal, external and inter-dependency issues. In Ronis' opinion, such inter-play of domestic and foreign affairs would affect the way cyber-security issues are viewed and handled. As such, cyber-security issues have to be considered along with the impact they might have on the welfare and security of the entire globe—a holistic world-view.

Ronis stressed on the need to understand the complex systems that cyber-communities are dealing with. The most important characteristic of complex systems to know and remember is that they can rarely be controlled. Moreover, it was highlighted that complex systems could only be "influenced" if, and only if, we understand them thoroughly. This is problematic for communities that are tasked to make predictions of the future as it implies that complex systems cannot be fully controlled and there are limits to what we can learn or know with any precision. Ronis thus commented that "we can predict with probabilities but not with certainty". Unfortunately, a majority of policymakers continues to focus their efforts on predicting the future and controlling the "complex systems" of the "real world".

Finally, Ronis concluded with findings from her work on the Project on National Security Reform in the United States. It was noted in particular that hyper-accelerated learning processes, foresight tools and all-of-government solutions have to be synthesized to improve decision-making processes. There is also a need to break down governmental stovepipes and create the mechanisms for complex systems thinking and foresight. It was thus argued that if we hope to be successful in tackling cyber-security challenges and threats, a similar synthesized and whole-of-government approach has to be considered.

WELCOME REMARKS

Cung Vu delivering his Welcome Speech on behalf of the GFF.

Cung Vu, co-organizer of the workshop, spoke on behalf of the Global Futures Forum (GFF) and welcomed participants to the workshop.

The workshop was organized with the need for experts of various sectors and countries to address pressing cyber-security concerns together. Vu stressed that international exchange of ideas and collaboration is crucial to the understanding and handling of cyber-security matters as they are often trans-national, diverse and complex in nature. The recent hacking (4 July 2010) of iTunes' Application Store and the complete shutdown of websites belonging to South Korea's (6 July 2010) key government and commercial organizations, for instance, were cited as indications of the diversity of cyber-attacks and level of destruction which cyber-attackers could potentially inflict in the near future.

To further underscore the importance of public-private sector cooperation on cyber-security management, Vu highlighted the impact that a computer virus attack (4 July 2010) had on the websites of the United States Treasury Department, Federal Trade Commission and Transportation Department. In this instance, various affected websites were benumbed by the virus and served as a crucial reminder of the consequences and implications that cyber-related threats would potentially have on homeland security. Vu also added that cyber-threats very often have a long lasting impact and highlighted for audience the danger posed by violent radical material distributed online.

In light of the broadness of cyber-threats both as a discussion topic and an emerging security risk, Vu encouraged participants to consider the range of measures and solutions that will address the challenges at hand and promote collaboration among organizations and states. In conclusion, it was stressed that a regional and collaborative approach to cyber-security is critical in countering and mitigating the broad impact of cyber-crimes and attacks on societies.

Kumar Ramakrishna delivering his Welcome Remarks on behalf of the CENS and RSIS.

Kumar Ramakrishna, co-organizer of the workshop and Head of the Centre of Excellence for National Security (CENS), welcomed on behalf of Dean Barry Desker of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU), Singapore, participants to the workshop. It was agreed that cyber-security is a broad field with varying implications for different sectors, organizations and even countries. Ramakrishna highlighted that, as a constituent research unit of the RSIS at NTU, CENS seeks to produce research that is both scholarly and policy relevant. As part of the research process, CENS understands that networking internationally is crucial in dealing with pressing national security challenges. This is especially so in today's globalized security environment where threats are inter-connected in complex ways that are not always easy to ascertain or discern. It is in this spirit of multi-national, multi-disciplinary and multi-sector collaborations that CENS has jointly organized the cyber-security workshop with distinguished colleagues in the GFF's Community-of-Interest on Emerging and Disruptive Technologies.

It is hoped that the discussion and networking session presented by the two-day workshop would lead to mutually beneficial and important action plans and policy outcomes. Ramakrishna stressed the workshop should mark the beginning for collaborations on cyber-security issues. Participants were thus urged to actively contribute and deliberate on ways or best practices to improve the security and resilience of cyberspace.

WELCOME ADDRESS

Peter Ho delivering his Welcome Address.

Peter Ho, Head of the Singapore Civil Service and Permanent Secretary for National Security and Intelligence Coordination, delivered the welcome address. He noted the timeliness of the workshop in creating the platforms needed to raise awareness of and consider the possible responses to the challenges of cyber-security. The Internet Revolution is like a double-edged sword in that while, on the one hand, it has brought about widespread socio-economic benefits to even the most remote corners of the world, it has on the other hand also empowered those who seek to destroy and disrupt. As such, regional and international cooperation is necessary in the tackling of cyber-crimes and attacks which are often trans-national in nature.

The range and frequency of cyber-attacks have broadened and increased in recent years. Mr. Ho mentioned, for instance, that businesses globally have, in a 2010 State of Enterprise Security Study conducted by Symantec, rated cyber-crimes as the greatest threat to their security. It was also added that the May 2007 Distributed Denial of Service (DDoS) attacks against Estonia serve as a reminder that cyber-attacks are not confined to just individuals or ogranizations and that countries and key state infrastructures can be targeted as well.

Of late, violent extremist groups and individuals seem to have increased their outreach activities and be planning attacks online. This is a worrying trend as coupled with the rapid advances in Info-communication Technology (IT), whereby anyone with a Wifi-enabled phone for example is capable of transmitting information to the cyber-community, it calls for changes in the way governments and mainstream civil societies conduct their counter-radicalization and outreach efforts. In response to the possible impact that online violent extremists views and activities might have on youths, the Islamic Religious Council of Singapore and several Muslim Singaporean scholars have taken the initiative to debunk radical ideas and respond to religious queries through the creative usage of websites and Web blogs.

In view of the growth of IT as both an opportunity and challenge, Mr. Ho shared that Singapore has implemented two key National Infocomm Masterplans to safeguard cyberspace transactions and at the same time harness the economic potential of IT. In general, the two Masterplans are built on four key strategic thrusts. They are: (i) to harden Singapore's info-com infrastructure and services; (ii) to enhance info-com security competencies; (iii) to cultivate a vibrant info-com security eco-system; and (iv) to advance international info-com security cooperation. The Cyber-Watch Centre and Threat Analysis Centre were set up, for example, to strengthen the capability of Singapore's public sector to mitigate cyber-security threat.

Besides efforts to enhance the public sector's situational awareness and ability to respond to cyber-incidents, Singapore also invests in information security research and education as part of a wider effort to enhance info-com security capabilities. The establishment of the Association of Information Security Professionals (AISP) serves as a case in point where Singapore's public and private sectors jointly collaborated to transform info-com security into a recognized profession and to groom competent info-com security professionals. Over and beyond the measures taken to harden Singapore against cyber-attacks and enhance info-com security competencies, steps have also been taken to ensure that vibrancy in the info-com industry is not stifled by the need for security measures. For example, students are encouraged to learn about cyber-safety and security through fun and educational online games.

In conclusion and given the borderless nature of cyber-attacks, Mr. Ho underscored the need for regional and international collaboration on info-com security. On this note, both speakers and participants were urged to identify new cyber-threats and to develop strategies for cyber-security management from a multi-national, whole-of-society and multi-disciplinary perspective. It was also hoped that discussions held during the workshop would lead to joint projects and initiatives to anticipate, guard against and mitigate the impact of cyber-attacks.

KEYNOTE PRESENTATION
Securing Cyberspace: Priorities and Challenges

Ruth David speaking on the impediments and challenges to cyber-security.

Ruth David spoke on the impediments and challenges to cyber-security.

According to David, cyberspace was coined 25 years ago by William Gibson, a science fiction writer, who had also anticipated its inherent borderless and complex quality. In particular, it was foreseen that computer-mediated communication will replace direct face-to-face interactions. The focus on cyber-security has thus far been on the hardening of hardware against attacks and from a "computer security" compliance standpoint. In David's opinion, it is the human aspect that complicates cyber-security and that is often difficult to address.

It was noted that cyber-activities are no longer restricted to person-to-person computer-mediated communication. In fact, cyberspace has become the infrastructure, platform and network that states, organizations and individuals build their administrative, business and social functions on. David argued that, given the level of prominence that cyberspace activities and interactions have in societies and everyday living, cyber-security has to move beyond setting compliance standards and the mere securing of "bits, bytes and wires"—hardware protection. It is also imperative that security policymakers and professionals recognize that nothing remains static in cyberspace and changes occur very constantly. Therefore, solutions to counter cyber-threats have to be developed in sync with the pace of change and that will be readily taken up by end-users (the everyday Web-users).

In a recent article by The Economist, cyberspace is listed as the fifth domain of modern warfare alongside such conventional battlegrounds as land, sea, air and space. The article suggested the possibility of going into battle without the need for anyone to physically move beyond the confines of his/her computer keyboards. David, however, cautioned that such a perspective causes us to view cyberspace and its technologies as the ultimate standoff weapon with the potential for people to create problems from great distances. This abstract notion, she argued, leads to some of the challenges we faced currently in cyber-security and the inability to derive useful policy frameworks that could promptly deal with emerging cyber-threats.

The stance towards cyber-security is, in general and to date, not unlike existing approaches towards physical border protection. David noted that the emphasis by most nations, at least for the United States, is to prevent "bad people or things from entering the country". However, at the pace at which the cyber-community evolves, operates and the amount of businesses that are dependent on the Web for their daily operations, it would be a difficult and impractical task to block all transactions and movements on cyberspace. A more important and balanced approach would be to seek ways to secure and restore our transactions against disruptions and post-attacks respectively. It was put forth that such an emphasis would push us to strike a balance between cyber-security and operational requirements, thereby enhancing cyber-resilience.

In closing, David listed a gamut of cyber-threat sources that could affect the way cyber-security is managed by countries. The range of cyber-threat motives varies dramatically from people who simple want to make use of cyber-tools to disrupt a nation's military operations to folks who simply want to gain economic advantage through the stealing of intellectual properties and identities. What is crucial from both a policy and operational perspective is how a similar deterrent theory might be developed for cyber-security that is highly flexible to changes, raise the cost of entry for the adversaries and allow for the restoration of cyber-transactions at the speed of light. It was also stressed that while cyber-threats might be universal, it is still possible for countries to develop measures to address localized cyber-security breaches and problems. Nevertheless, it was reiterated that given the inter-connected and borderless nature of current day's transactions and cyber-crimes/attacks, collaboration among countries and with the private sector is crucial in the securing and building of cyberspace and resilience.

PANEL 1- CYBER-THREATS: AN OVERVIEW
Overview of Cyber-Threats, Criminal and Terrorist Online Activities to Date

The Honourable John Grimes sharing his thoughts on cyber-security.

The Honourable John Grimes presented his observations on cyber-security and its current status based on his experience and empirical evidences.

In Grimes' opinion, the two concepts crucial to our understanding of cyber-security are those of "trust" and "attribution". The signing of bilateral agreements is an example of how mutual trust could be built among countries. As for the sources of cyber-threats, they can be attributed to both "insider" and "outsider" attackers. Grimes stressed that cyber-attack from someone within an organization remains a major threat to both governments and private organizations. It was also added that it is often difficult and a challenge to detect insider attacks (and attackers). In contrast, an "outsider threat" could usually be traced to an external software or application that has been installed by an enterprise. The challenge, in this case, would be to determine what has been encrypted in the software and remove the embedded threat.

Data and information protection is not a new topic. Grimes shared that, from as early as the 1980s, the Security Council in the White House has written policies and worked in collaboration with the public to protect data and information. Despite the headstart on data and information protection, challenges continue to exist and formulating policies to address this area of concern remains a difficult feat. This is due in part to the "Big Brother Syndrome" which has both the U.S. congress and the public perceiving that the Security Council would screen every detail of their information. Thus, there is a tendency for the U.S. congress to view the entire movement to protect data and information with some degree of pessimism. Moreover, there is also the added difficulty in building the infrastructure needed to bar access to personal or classified information into a network that was first and foremost created to facilitate the transfer of information.

The scale and range of cyber-security threats that confront us today is huge and extensive. Grimes illustrated through case studies, for instance, that the network of the U.S. Department of Defense (DoD) experiences six million attacks a day. Likewise, Estonia and Georgia suffered from massive Botnet attacks and network disruptions within a short span of two years. The attacks are not only against states but also against commercial establishments.

According to Grimes, McAfee has estimated in a report that companies have lost close to US$ 1 trillion worth of intellectual property from data theft alone. Over and above the frequency of such cyber-attacks, is the problem of attribution. The recent 4 July 2010 cyber-attack against the United States, for example, were reportedly traceable to both North Korea and the United Kingdom (UK)-based sources. In such a scenario, it is difficult to ascertain definitely who the adversary is and the attacker's country of origin due to its borderless nature.

In closing, Grimes stressed that, in the face of rising cyber-threat, information sharing and situational awareness is crucial to the U.S. government to keep up to the pace of the adversaries. In his opinion, collaboration on cyber-security is unfortunately still very much a work in progress. As final takeaway for participants, Grimes emphasized the need for Internet users to be educated on information protection as well. It was underlined that while there is no one-bullet-proof solution to ensure total cyber-security, a range of measures could be taken to reduce vulnerabilities.

CYBERSPACE – TAMING THE WILD WEST

John Savage providing participants an overview of current cyber threats and challenges.

John Savage gave a general overview of what the Internet constitutes, as its attending cyber-threats and shared with participants the way forward in the face of such threats.

In Savage's opinion, cyberspace could be treated as a "Wild West" of sorts where hackers could be likened to "gunslingers", and computers to "towns". Thus, the challenge of the Wild West is to develop "sheriffs" who would "slap a badge on a hacker" and protect the towns under their charge. The Internet, defined by Savage as a "collection of networks", is in itself a kaleidoscope of opportunities and threats. It has, for instance, facilitated the freedom of expression while at the same time accentuated cultural differences. It has also exposed the vulnerabilities of critical networks and made them prone to cyber-attacks. According to Savage, the U.S. Department of Defense (DoD) suffers an average of 600 million cyber-attacks to its computers daily. Naturally, networks belonging to such critical infrastructure as power grid, financial and banking systems have become extremely vulnerable targets to external attacks. In this regard, it was opined that the United States is in an especially vulnerable state because it is not only the most wired nation on earth but its cyber-defence is also not on par with its level of connectivity.

The most dangerous cyber-attack tool to date is Botnets—networks of infected computers. According to Savage, Botnets is the preferred cyber-attack tool as they are not costly to attain and have a highly destructive impact on networks and systems. Moreover, Botnets could be easily "manipulated" to perform different functions, and therefore, inflict various types and degrees of damages. It is also often difficult to suppress the spread of, or remove Botnets entirely as their command and control hosts are not fixed and they can change hosts very easily. As such, this makes Botnets one of the most powerful cyber-threats. As an illustration of the harm that Botnets can inflict, Savage shared with participants that major banks and companies registered more than 70,000 acts of compromise by the Zeus Botnet attack in 2009. The Zeus Botnet has not been completely wiped out and, in fact, "Do-It-Yourself kits" to create Zeus Botnet is now available for purchase off the Internet. As for the risk that Botnet can pose to national security, it was stressed that the Botnets have the potential to, for instance, destroy nuclear power plant cooling systems and have previously disabled military Internet services and banking clearance systems.

According to Savage, there are two key challenges to cyber-security. Firstly, he mentioned that even if nations improve their defences and devise protective measures, attacks cannot be entirely prevented. The race to stay ahead of hackers will continue to persist and, as such, protective measures taken up by states often turn out to be insufficient by the time they are implemented. Secondly, in reality it is difficult to decide the appropriate time to retaliate against a cyber-attack. In fact, before any state or organization could conduct any "external retaliation", Savage emphasized that the following preconditions are crucial: (i) attribution with very high assurance; (ii) a recognition that collateral damage will be limited; and (iii) an understanding of the potential domestic repercussions.

In view of the challenges, Savage proposed the following as ways to enhance cyber-security: (i) commit to serious study of cyberspace; (ii) encourage vendors to continue improving security; (iii) work on necessary domestic legislation; (iv) increase engagement and collaboration with international partners; (v) encourage education and public discussion; and (vi) fund innovative research and policy development.

In conclusion, Savage said that cyberspace is a complex new medium which poses a number of challenges. He stressed that addressing such challenges strongly requires decades of research, policy development, legislation and international negotiation.

EVOLUTION OF CYBER-THREATS

David Aucsmith providing participants rare insights into the technical aspect of cyber crimes.

David Aucsmith provided participants rare insights into the technical aspect of and implications for cyber-crimes from a software developer's point of view.

According to Aucsmith, 80 per cent of the world's critical infrastructures in cyberspace are provided by private commercial enterprises. However, their business is subject to numerous cyber-attacks due to their bandwidth and accessibility. He said that tackling cyber-threat is difficult because of two fundamental problems: (i) adversarial relationship; and (ii) inherent complexity. Although Bill Gates' Trustworthy Computing Initiative was devised in the face of increasing adversarial attacks, it was still extremely difficult to effectively counter the attacks due to a general poor understanding of the adversaries. Therefore, Aucsmith opined that a more feasible option would be to build an adaptable system rather than an absolute firewall.

In an effort to build an adaptable system to fight adversaries, sensors were developed by Microsoft to better understand and detect the adversaries. However, the effort did not yield as much results as expected and, thus, it remains a challenge to develop sensors that could outpace the adversaries temporally and spatially. To illustrate the capability of adversaries to launch quick and mass intrusions into networks, Aucsmith shared that around a week after the Blaster Virus attack, a Chinese cracking group called X-focus published an exploit tool that could be used by either the public or hackers' community to develop the Blaster worm. This occurred almost simultaneously after the virus attack was reported to Microsoft and it has delivered a counter-vulnerability patch to its clients. The Blaster Virus attack also exemplifies the complex interplay of plans and actions by security researchers, software companies and hackers in cyber-crimes.

While there is no one perfect solution to address all cyber-related challenges, a range of technological methods are available to detect, for instance, adversarial intrusions. In Microsoft's case, Aucsmith shared that one such method involves the utilization of search engines to detect suspicious activities. For example, search engines supported by Microsoft are programmed to detect and report searches on "How to hack into Microsoft programmes". Moreover, the company also maintains a reporting system which enables approximately 500 million Personal Computers (PCs) to report system crashes. Based on these crash reports, software companies will try to find a particular pattern, specifically the "strain", to establish the cause of the reported problems. Furthermore, the reporting mechanism is complemented with such exploit detection systems as "Traditional Honey Pots" and "Strider Honey Monkey" that gather information on and identify attackers and malicious websites respectively.

All in all, Aucsmith opined that cyber-defence is only as effective as our intelligence allows it to be. Intelligence, it was noted, could be improved by continuously developing sensors and conducting threat analysis. Besides intelligence, agility or adaptability is also a crucial trait for survival against existing and emerging cyber-threats. In conclusion, Aucsmith emphasized that "defence in-depth" should not simply be regarded as a bunch of different products. Instead, it should be a collective system in which signals sent from one part of an infrastructure automatically determines the movement of another part of the infrastructure without human intervention. In this regard, Aucsmith suggested three security actions to counter cyber-threat: (i) deploy patches quickly; (ii) update your software to the most current version; and (iii) move quickly to 64-bit architectures.

DISCUSSION

In response to a participant's question on the ability of software companies to track an adversary thoroughly, a speaker agreed that it would be extremely difficult to ascertain specific information such as the Operating System (OS) or Internet Protocol address of an adversary. Software companies generally track an adversary based on information which is already available on the Net. It was also added that in crash analysis system reporting, all personal identification information are removed. Thus, software companies can only get a rough idea of how the system crashed. More accurately, the tracking of adversaries refers to the detecting of malwares and attacks against a system and not the hunting down or screening of individuals per se.

As for the threat of state-sponsored cyber-crimes, another participant wanted to know if the panellists had known or encountered real examples where links between hacker groups and governments could be established. A speaker answered that while credible evidences do exist and suggest connections between some governments and hacker groups, the connection is difficult to establish definitely. The difficulty in ascertaining the links also lies in the blurred line between state-sponsored and state-tolerated cyber-activities.

Finally and in relation to state-tolerated cyber-activities, the panellists were asked to comment on the possibility that hacking be seen as form of a civilian protest. As such, should the state display tolerance to such a form of protest? A speaker replied that whether it is a criminal offence or not depends on whether the hacker has broken the law. Another speaker also added that as there is currently no fixed definition on what constitutes a "criminal act" or "act of war" in cyberspace, it would be difficult to establish definitely if hacking should be seen as a criminal offence or a form of civilian protest.

PANEL 2- TECHNOLOGICAL AND LEGAL TOOLS
Countering Terrorism on the Internet – Technological and Legal Tools

Alexander Lim sharing with participants the Interpol's approach to cyber-security.

Alexander Lim delivered a presentation on cyber-crime from the perspective of an international law-enforcement agency. Participants were given a panoramic view of the issues that arose when Interpol tries to tackle cyber-terrorism. Moreover, Lim also briefed participants on the set of unique tools that Interpol utilizes to support its member countries as well as the on-going developments in the field of cyber-security.

Lim noted that there has been a change in terrorist communication methods and—since 2004—terrorists have shifted from face-to-face to online communication. The 2004 Madrid Bombing, for example, was reportedly to have been inspired by a document posted on an extremist website. In addition, two men involved in 2004's Operation Crevice were reportedly to have also kept in touch with each other through the Internet. These examples are illustrations of the communication trend among terrorists and how online interaction has become the preferred mode of information exchange.

Numerous radical groups, including prominent groups such as the Al-Qaeda and Hamas, have an online presence today.

According to Lim, the managers of such radical websites are sensitive to their audience's sentiments and often react according to their support biases. These websites are mainly monitored for their content, specifically terrorist training materials, indications of online recruitment and terrorist funding activities. Lim stressed that to deter the growth of radical websites, online communication among terrorists and their sympathizers have to be hindered. Measures to deter or hinder interactions online could range from the blocking of Internet Protocol addresses to the shutting down of websites entirely. However, this can only be accomplished when there is cooperation among police agencies and mandates are in place to govern the monitoring of websites. As for the Interpol and when it comes to website monitoring, Lim noted that its attention is largely focused on the surveillance of interactions between extremist websites and their audiences.

The Interpol has sought to help its member countries tackle cyber-crimes and related issues through the application of its existing policing tools especially in the monitoring of suspicious online activities. Interpol policing tools, it was added, are developed with the intention of facilitating international cooperation through: (i) the establishing of networks of counter-terrorism and cyber-crime investigators; (ii) information sharing; and (iii) joint operations. Currently, the Interpol is attempting to integrate the databases (DB) of different countries to improve information sharing on criminal profiles and activities. All these efforts, however, work at utilizing either the Interpol's or its member's existing law-enforcement tools and technologies to counter current and emerging threats. Lim noted that the Interpol's stance is that, instead of investing heavily in mostly unproven technology, more efforts should be devoted to the training of law-enforcement personnel to better utilize existing tools and services to combat crime and counter-terrorism on the Internet.

There has been much debate, for instance, over the supposed benefits of Cloud Computing and how it might facilitate efficient information sharing among its users. Cloud computing, as it was explained briefly, is an Internet-based development that allows users to run programmes and retrieve data from a common "cloud" instead of a stand-alone computer. However, Lim shared that from Interpol's and a law-enforcement perspective, cloud computing poses several challenges. For one, it complicates police investigations and the gathering of evidence in other jurisdictions especially when information is stored on service providers based in different countries. Hence, a simple data and content retrieval could only take place when there is judicial clearance, cooperation and coordination among foreign law-enforcement agencies.

In conclusion, it was reiterated that it would be more practical an approach to train law-enforcement personnel to better understand the uses of existing tools than to invest heavily on new tools with poor credibility just to catch up with the pace of technological developments. Lim stressed that existing tools have the potential to be further developed and refined to suit the needs of law-enforcement agencies to fight online terrorist activities.

CONTROLLING THE CYBER-THREAT

John Savage explored in his presentation the dynamics between technology and policymaking. In particular, Savage considered the various types of computer attacks and its implications on national security policies. It was stressed that good policy is informed by technology and vice versa. As such, cooperation among technologists, policymakers and even economists is crucial in the securing of cyberspace against attacks.

The main challenge is perhaps the control of the cyber-threat itself. Indeed, it is a mammoth task trying to control the malicious use of the Internet. In particular, Savage highlighted the difficulties in both the utilization and development of existing tools and technology respectively to harden computers and networks against attacks. Moreover, the challenge is global in nature and thus, national laws and international agreements are needed before the problem could be addressed. Even then, it was opined that economic incentives must be in place for cyber-security solutions to sustain and remain viable.

Savage asserted that it is crucial to understand the dialectics between technology and policymaking. The key argument is that technology influences policies just as much as policies affect the way technologies are developed. As such, both technologists and policymakers should inform one another of their needs and concerns over cyber-security before any strategies are developed. In a similar light, Savage underscored the importance for policymakers to be well informed of the security measures that are already in place and taken up by the industry before deciding which direction to take to counter cyber-threats. Essentially, it voices down to a question of security ownership and a thorough understanding of the sources of insecurity.

According to Savage, there are five important types of computer attack and they are namely: (i) buffer overflow; (ii) SQL (Structured Query Language) injection; (iii) Cross-site scripting (XSS); (iv) Distributed Denial of Service (DDoS); and (v) Domain Name Server (DNS) redirection. Savage explained that buffer overflow is a problem that occurs when a programme stores more data in its memory storage than expected and, as a consequence, manipulates stored data and any other running programmes. A way to counter this type of attack is by the enforcement and application of a basic safety property known as "control flow integrity", which prevents a programme from deviating from its designed behaviour. As for SQL injection, this occurs when inputs, database queries for instance, reveal important information hidden in the network. Savage suggested that this type of attack be prevented by limiting the number of queries that the users can run.

In contrast, XSS attack occurs when someone injects HTML commands into a client website to extract classified information. According to Savage, Symantec reported in 2007 that 80 per cent of security vulnerabilities were due to this form of attack and to prevent it, requires a careful parsing of computing commands. DDoS attack occurs when compromised computers saturate or flood a targeted computer with, for example, multiple requests and prevent legitimate users from accessing a computer-based resource or service. Savage said that while it is difficult to defend against some DDoS attacks, it is still possible to control the rest. Lastly, DNS redirection occurs when DNS cache is "poisoned" by incorrect Web address that diverts users to unintended contents. Savage said that one way to counter this attack is for users to accept update of addresses' request only from trusted parties. He added that the prevention of DDoS attack also requires similar authentication process and integrity checks.

In closing, Savage offered some suggestions for consideration on the way forward for cyber-security. Firstly, technologists, policymakers and other parties related to cyber-security should develop partnership and work in collaboration. Secondly, all parties should be informed about available technological solutions, including their weaknesses. Thirdly, it should be realized that cyber-security is global in nature and requires long-term solutions. Finally, Savage noted that it is important to invest a substantial fraction of available resources into the mitigation of cyber-attacks.

CLOUD COMPUTING SECURITY – THE SOFT SPOT

Anthony Lim presenting on the perils of online information exchanges.

Anthony Lim analyzed in his presentation the concept of cloud computing and put into perspective for participants how cloud computing has been manipulated for cyber-criminal activities.

Of late, cloud computing technology is considered a flexible, cost-effective and innovative delivery platform for providing business or IT services over the Internet by many institutions. Albeit the huge benefits that cloud computing have brought about, including minimizing capital expenditure and increasing computing power, it has brought along several negative side effects. There are three key security considerations to take note of in cloud computing. Lim listed them as **Confidentiality**, **Integrity** and **Availability**. Confidentiality refers to the protection of data, integrity refers to the compromise of data and availability refers to the ability of firms to deliver services to their clients. From experience, Lim found that individuals and firms tend to focus excessively on availability and often forget the importance of maintaining confidentiality and integrity.

Lim opined that the main problem with cloud computing lies in people's complacency over data protection. Often, most firms and individuals are satisfied with just having basic security features like firewalls and Intrusion Prevention Systems (IPS) installed into their networks. Some might conduct an audit on their systems once a quarter with pen testers, network vulnerability scanners and encrypting their data with Secure Sockets Layer (SSL). However, Lim warned that there are still some areas that cannot be covered with the aforementioned tools especially under a cloud computing system where applications and resources are shared via the Internet.

It was argued that cyber-attacks can and do occur even in a seemingly secure environment. For example, Lim noted that an online recruitment company's firewall and IPS log failed to detect that around 100,000 resumes submitted by its registered applicants have been leaked to a third-party company. Similarly, a hacker managed to steal 130 million credit card numbers from supposedly secured financial sites in 2009. These examples clearly show that hackers are capable of carrying out a software attack even in a cloud computing system. It was also added that past incidences have also shown that the attacks are not limited to software and hackers are known to have carried out attacks on applications operating in a cloud computing environment as well. Lim shared that applications can be "crashed", "compromised" and "hijacked" through unconventional hacking methods to perform tasks for an unauthorized user or reveal crucial information to hackers.

As a case study, Lim described how a seemingly normal crash experienced by an online magazine subscription webpage in turn revealed its subscribers' information. This wealth of data could potentially be used by hackers for criminal purposes. Likewise in another case, despite the security assured by an online hotel reservation website, its registered clients' information was easily attainable through a simple tweak in the "secured-https" address field. These examples clearly illustrate how information and data can be easily attained and basic security features can be bypassed to reveal crucial information to hackers. Lim opined that these application security problems exist because most software developers do not pay much attention to application security. That said, IT security professionals often lack experience in application development as well.

In conclusion, Lim reiterated that we could not expect applications to "defend themselves" and assume that firewalls will detect or deflect all cyber-security breaches. It was asserted that the best ways to prevent an application attack is to ensure the robustness of the application and bridge the gap between software development and information security. Lastly, Lim argued for the need for Quality Assurance (QA) security testing to be carried out in an integrated and strategic manner.

DISCUSSION

A participant questioned whether the case studies raised by the panellists constitute to open source information exploitation or hacking. The information revealed through the parent directories and hotel reservations pages seemed to suggest that hacking has taken place as well. In response, a panellist stated that a simple and creative use of Boolean Logic to attain such data only show how easy it is for information to be compromised and exploited by hacking tools. There is, therefore, a need to educate programme writers of such possible violations and abuses. As a matter of fact, it was added that hackers are now able to develop their own methods to pass through application firewalls. This is usually done by hacking the "business logic", which in the panellist's opinion in today's cyber-security environment, is becoming more than merely an open source information exploitation.

With regards to cyber-terrorism, a participant wanted to know if the shutting down of extremist websites would lead to any violent reactions or retaliations from the adversaries. A speaker answered that thus far website managers react by re-uploading new extremist websites on different servers and Uniform Resource Locator (URL). As a follow up, speakers were then asked if their respective countries' law-enforcement agencies intend to put in place any measures to counter online radicalization. A speaker answered that many law-enforcement agencies around the world conduct programmes and researches to monitor the development of radical websites. However, initiatives or specific measures to counter radical websites have yet to be devised at an international level.

PANEL 3 – IMPLICATIONS FOR HOMELAND SECURITY
Implications of the Evolving Internet

Lori Lessner presenting on the implications of the evolving internet to homeland security.

Lori Lessner began her presentation by stating that the Internet has transformed the way the world plans, shops and communicates; with Web 2.0 having facilitated this evolution, creating a user-generated, interactive arena. This environment, she explained, has been enabled by converging technologies that are faster, cheaper, smaller, easier to use and which are accessible everywhere. With these readily available technologies, global relationships are able to form instantly across a plethora of platforms which include: Social Networking Sites (SNS), blogs, forums, online games, virtual worlds and augmented reality. Lessner added that the use of these platforms has also enabled individuals to form circles of trust by joining others with similar interests in organized and functional online communities. Thus, she argued that the Internet has become social by default—being first and foremost a social tool, with data being secondary.

Lessner suggested that while more and more people have begun to feel comfortable using the Internet, those feelings are for an outdated Internet. Unlike many adults who use e-mail as their preferred communication medium, today's youth prefer text messaging because it is instant. Some even refer e-mail to "snail mail", a term once reserved for mail delivered by the postal service. She then added that social media is more than mere entertainment or a way to connect with friends. Rather, it has been recognized by individuals and governments worldwide to be a critical outreach tool. It was argued that the Internet has evolved to a point where it has empowered participation in politics and revolutionized the formation of personal relationships. Lessner pointed, as an example, to the case of China, which on its own has nearly 10,000 SNS and approximately 400 million Web-users; this is more than the entire population of the United States. She also suggested that social media matters a great deal today, particularly in a country like China, which has been harnessed into an effective political outreach tool. However, she cautioned that while the Chinese government may be using the Internet for outreach purposes, they have also expressed concern that unfiltered speech threatens national stability. Due to these concerns, China heavily monitors the Internet and maintains a list of hundreds, if not thousands, of banned search terms. Yet even with these bans in place, Chinese citizens continue to work around these obstacles, playing a game of cat and mouse at times, by using homonyms to circumvent such monitoring.

The next example that Lessner pointed to was Iran, who unlike China, has been less adept at controlling information. Specifically, she singled out the 2009 election where opposition candidates used SNS to reach out to the population. It was highlighted that the Iranian population is very young and Web savvy. As such, the use of social networking tools was a very effective way to reach out to Iran's voters. After the election and while the government was claiming that it had won, the population and the opposition used SNS to organize and coordinate protests as well as inform the rest of the world what was going on in Iran. According to Lessner, by the end of the election, the Iranians had sent more than two million tweets—signalling that the government was unable to control SNS effectively. While it has been a year since the election, it was mentioned that Iranian authorities continue to intimidate their population using a number of tactics—one of which requires Iranians to log into their Facebook accounts at the airport for inspection.

Lessner then moved on to discuss how violent extremist groups have made use of the Internet. Specifically, she focused on how violent extremist groups have been using the Web to reach out to women since around 2000 and 2001. A site maintained by a violent extremist group, for example, describes how women should raise children to join the jihad. Lessner also pointed to a website developed by Hamas which details a step-by-step plan of action instructing women how they could carry out suicide attacks. The Al Qaeda has also reached out to women in a similar fashion with the wife of Alzawaheri publicly endorsing female suicide bombing both on the Aljazeera television channel as well as online.

Lessner concluded by arguing that violent extremists use the Internet to lure disenfranchised individuals resentful of globalization and who are resentful of western values. However, while these factors may remain the same, there is now a shift taking place in which violent radical groups are abandoning recruitment videos which opened with a call to prayer. Instead, they are turning to rap videos which display beheadings and other graphic images to appeal more effectively to resentful youth.

ONLINE INFLUENCE, INDOCTRINATION AND RECRUITMENT

Sarah Womer speaking on the correlation between online and real life terrorist activities.

Sarah Womer began her presentation by asserting that Al Qaeda's presence online is not a new phenomenon. Rather, it is the tactics that they are using that are evolving and are considered new. According to Womer, Al Qaeda's online activities pre-date September 11 and even at that early stage it already has an active and robust presence online. It was noted, for example, that Azzam.com was developed as early as 1996 with its content available in 27 different languages and the website maintained by an office in London where individuals were able to send cash cheques to. It was emphasized that while the threat of cyber-terrorism was important to pay attention to, the phenomenon of online indoctrination must be monitored more closely in that such indoctrination can potentially lead to real-world attacks.

According to Womer and based on her observations of multiple ideologues circulated online, patterns of increased rhetoric and online reporting of clerics' activities could indicate an impeding attack. By asking the following questions of "whether there is a consistent pattern", "if this pattern is building up to a crescendo" and "whether or not this crescendo will be followed by action", analysts may be able to determine when and generally from where an attack might take place. Specifically, she suggested that clerics who are acting as online influence agents should be paid close attention to. It was added that influence agents' online activities may be direct and/or indirect. An example of a direct effort were the 2008–2009 global Voice Over Internet Protocol (VOIP) conferences and seminars where Anwar al Awalki reached out to selected audiences, including the Christmas Day bomber, prior to the 2009 Fort Hood shootings.

Womer suggested that the next generations of Al Qaeda's recruit potential are currently being courted from a variety of milieus. Indeed, the Al Qaeda has utilized cultural specific websites and creatively used an assortment of languages to appeal to these potentials in their recruitment efforts. Through a series of examples, Womer illustrated to participants how various influence agents had via social networking platforms, Internet Chat Services, Blogs and discussion forums reached out to their target audience, if not recruits, from a variety of states including, but not limited to, the United Kingdom, Australia, Pakistan, Indonesia, Bosnia and Thailand.

The tracking, monitoring, and analyzing of online influence agents through open source research can yield insights into overall terrorist recruitment efforts and modus operandi. Womer opined, for instance, that if there was an online spike of information and propaganda from Anwar al Awalki in English, this would likely indicate a more directed effort at appealing to audiences from the United States, United Kingdom and Australia. This effort may also indicate a possible increase in English-speaking recruits who may act on the offered ideology.

In conclusion, Womer cited the need to avoid over generalizing when examining ideologues. In her opinion, there needs to be a closer examination of the online enemy in order to determine who they really are. Specifically, Womer stressed the need for a more in-depth examination of how the ideologues or clerics are recruiting on the Web.

SECURING PHILIPPINES' CYBERSPACE: CHALLENGES AND ISSUES

Nicolas Ojeda sharing with participants the Philippines' experience with cyber-attacks.

Nicolas Ojeda Jr. began his talk by stating that the number of Internet users in the Philippines has been projected to reach 30 million by 2012. He also explored how the term "cyber-revolution" affects the way information reliability and security are understood in the Philippines. Moreover, he also considered the impact that cyber-revolution has on Filipino value and how it affects the way information is acquired.

Ojeda noted that the concept of national cyber-security was recognized as an indispensable part of the Philippines' national security after the notorious "I LOVE YOU" computer virus, which was developed by a Filipino computer programming student, inflicted global damage that amounted to approximately US$5.5 billion. This experience highlighted the limited cyber-security and cyber-defence capabilities of the Filipino government, reminding all concerned of the country's continued vulnerability.

A case study highlighted by Ojeda involves the online communication efforts of Abu Sayyaf Group (ASG), who as a terrorist group has been exploiting social media for a range of recruitment and outreach activities in the country. Since 2007, ASG operatives have been uploading MP4 video files to YouTube in order to broadcast their less-than-benign intent. In particular, Ojeda pointed to an ASG fund-raising video entitled, "The Filipino Lions are Coming", which has effectively helped the ASG garner an undisclosed amount of money from foreign donors.

In another instance raised by Ojeda, specifically the January 2009 Red Cross kidnapping incident, it was also shown that the ASG is equally capable of using e-mail services to broadcast the status of their victims. They were also able to publicize their demands to the Filipino government and the world through communication with the media by satellite and cellular phones. At a tactical level, Ojeda opined that the Armed Forces of the Philippines recovery of the satellite and cellular phones used by the ASG also served as an indication of the adeptness of the ASG to utilize modern communication technologies for their field operations in the Sulu and Basilan, Southern Islands of the Philippines Archipelago.

The ability of terrorist groups to use Web-based technologies to communicate their group's demands to the world despite the range of electronic defensive measures in place, points to the Philippines' lack of a comprehensive cyber-security plan. Ojeda explained that presently, the government has no training mechanism to develop and certify a significant mass of local "cyber-security experts". Subsequently, it has to depend on foreign universities and institutes to train personnel assigned to cyber-security units.

While Ojeda acknowledged that the government has undertaken efforts to introduce and establish the cyber-security agenda, he noted that there is still a general lack of awareness and understanding by key government and private stakeholders over the seriousness and impact of both current and emerging cyber-threats. This impedes any on-going and long-term efforts at countering cyber-threats. Therefore, Mr. Ojeda argued in conclusion that it is necessary for the new government to assume a proactive role in improving the country's cyber-security capability. Ideally, this should be pursued by enacting a robust cyber-security law and implementing or at least improving the existing National Cyber-Security Plan.

DISCUSSION

A member of the audience questioned the role that face-to-face indoctrination has in the radicalization process over online interaction. In response, a speaker answered that this has changed over time with groups like the Al Qaeda relying more and more on the online side of the radicalization process. It was also opined that face-to-face interaction would become less important as technology and SNS advance with time.

The panellists were also asked if there is a correlation between the amount of messages posted by individuals on radical forum websites and their willingness to move from talk to actual violence. One of the panellists shared that there have indeed been cases where a noted increase in cyber-activities was eventually followed by or matched with an actualization of real-life violence. With this in mind, the speaker suggested the closer examination of individuals whenever there is a noted spike in online extremist activities.

Finally, the panellists were asked to comment on the possibility of virtual platforms like Second Life being used as practice areas for terrorism. A speaker noted that there have been reported cases of people play-acting as terrorists on Second Life. However, it is still not clear if this suggests a change from physical to virtual terrorist training grounds.

PANEL 4- CYBER-SECURITY FROM A "REAL-WORLD" PERSPECTIVE
Securing Banking Systems Against Financial Crimes and Terrorist Financing

Gunawan Husin speaking on the impact of cyber crimes on banking systems and regulations.

Gunawan Husin focused in his presentation on the emerging threats and trends in financial crimes as well as possible initiatives to combat these risks. Despite being one of the most stringently regulated industries, the financial sector faces increased challenges in pre-empting and preventing the occurrences of financial crimes. Husin noted that while the sector is still struggling to regulate conventional, traditional banking services, criminals are already exploiting new financial products and services.

Money laundering and terrorist financing are two key areas that the financial sector must guard against. Money laundering involves the process of filtering proceeds through one or more financial transactions to give it legitimacy. Historically, money laundering is investigated as part of a wider drug-trafficking movement. The scope of money laundering is broader today with a range of proceeds derived from criminal activities being entwined under this rubric. In contrast, terrorist financing involves the process of raising, storing, moving and using funds for the purpose of terrorist acts. The key challenge for banks in this area is therefore to ensure that not a single dollar that is deposited is re-channelled for terrorist activities.

Moving on to the legal and regulatory perspective, Husin highlighted that the Financial Action Task Force (FATF), inter-governmental body, was set up in 1989 to develop and promote guidelines and international standards for financial institutions. The Asia Pacific Group (APG) on Money Laundering is more relevant to the Asia-Pacific region. They have similar functions as the FATF assessing the compliance of members on money-laundering standards.

From a banking perspective, measures to combat money laundering and terrorist financing are causing financial institutions to put in place longer and more detailed processes to comply with industry standards and regulations. For instance, under the "Know Your Customer" (KYC) guidelines, banks are now expected to know who they have established banking relationships with. Banks are also expected to assess their risks before launching a new product by identifying beforehand who their potential customers are and classifying them into different categories such as politically exposed persons (PEPs). Husin added that other regulatory processes which must be complied with include the monitoring and maintenance of suspicious transaction reports on unusual transactions.

Despite all the measures taken by financial institutions to prevent money laundering and terrorist financing, the financial sector is still facing limited success. This is largely due to the fact that banks are usually not on an equal footing when it comes to their level of preparedness in combating money laundering and terrorist financing. Furthermore, running a compliance-risk management programme is expensive and requires banks to have adequate human, technological and financial resources.

Similar to the plight faced by most law-enforcement agencies tackling cyber-security issues, financial institutions have to confront the problem of dealing with different financial jurisdictions as well. For example, the Liberation Tigers of Tamil Ealam (LTTE) was only designated as a criminal organization by certain countries only as recently as 2006. This makes the monitoring of financial transactions across banks based in different countries problematic as what is considered illegal or criminal in one country might not be judged the same in another. As such, this also contributes to the lack of willingness by financial institutions in different jurisdictions to invest and keep a close watch on possible financial gaps that might be exploited by terrorists and financial criminals.

As for emerging areas of concern, Husin mentioned that for the financial sector there are already worries over the possible abuse of the newly introduced "mobile financial services" product. Similar to the "hawala" system, the product allows its customers to send money to overseas destinations through telephone companies. From a commercial perspective, this is a profitable business model. However, it also poses a security risk in that currently there is no mechanism and guidelines in place to monitor transactions and regulate the usage of this product. As such, there are concerns that the product might be misused for criminal and terrorism purposes.

Likewise, there are also raising concerns that both criminals and terrorists alike would resort to virtual banking to raise funds for their activities. Virtual currency, for instance, is a system of payment that allows its customers to change physical currencies to an electronic version for online gaming and purchasing purchases. This is the preferred mode of payment for criminals as they neither need to disclose their real identities nor figure how to bypass lengthy banking processes to attain funds illegally. Husin added that from a terrorist financing perspective, if one were to plan to raise funds today without making use of banks, a popular method would be to buy credit card account numbers from an online hacking forum. After which, the information could be used to enter online gaming sites and once the desired funds are raised, the proceeds are "cashed out" via the virtual currency system of payment.

The financial sector, being the first line of defence, will be under tremendous pressure to counter the possible abuse of online financial services and products for criminal and terrorism purposes. However, such an intense focus will draw attention away from the need for capacity building especially when banks have different levels of preparedness against a range of financial risks and security threats. Therefore, Husin concluded that to successfully combat and prevent money laundering and terrorist financing, political willingness and public-private partnerships are extremely crucial in dealing with this universal problem.

HARDENING AGAINST MODERN MALWARE; UPSTREAM INTELLIGENCE AND PROACTIVE SECURITY

Tyson Macaulay speaking on the vulnerabilities of current anti-virus software.

Tyson Macaulay began with the comment that, in general, policymakers often do not understand the technical aspects of information technology. His presentation is therefore focused on the technical perspective of the threat of malware. Macaulay noted that Bots-and-Not viruses are the biggest threat to the Internet, with professional Bot-Heads controlling millions of bots. When it comes to evading detection, modern malware is very successful at circumventing even the best anti-virus software available.

According to Macaulay, most anti-virus software is no more than 60 per cent effective at detecting and removing novel pieces of malware. It was also added that anti-virus software updates could hardly catch up with the speed at which malwares are reappearing and morphing. In fact, several new malware strains are highly capable of changing forms before it could even be detected. The irony of it all is, malware creators are known to have freely created and provided "security software" which removes all bots except their own creations.

Signature-based-threat-management tools have in Macaulay's opinion reached a "point of diminishing returns" in that they could no longer provide much added value to their users beyond what they have been originally designed to do. They do not only require massive processing power to run on personal computers and servers but also are not very efficient in "catching" many new malware variants. In view of the efficacy of signature-based-threat-management tools, it was proposed that a better course of action would be to share information on sources, destinations, ports and protocols—moving into a system where information is shared about known bad Internet Protocol (IP) addresses, domains and Autonomous System Number (ASN).

Macaulay mentioned that there are three parts to information sharing: (i) collection; (ii) aggregation and correlation; and (iii) distribution. Of the three parts, the third requires prompt action as information "decays" very quickly in value these days. As such, Macaulay stressed that the distribution of intelligence needs to be on a real-time basis for information to be of use. However, there is a problem of information source credibility. On the one hand, there is a need for intelligence to be distributed quickly to counter malware attacks. On the other hand, there is also a need to determine the credibility of the information source. Open source information comes with a great deal of variety in terms of its quality, veracity and credibility. Macaulay highlighted that there are about 1,600 large Internet Service Providers (ISP) and carriers in the world with an informal sharing network that is not regulated by any government. The lack of regulation, however, reflects the urgency of the matter and the market not wanting to wait for policymakers to figure out how to deal with the problem.

In view of the problems related to information distribution, Macaulay opined that there is a need to start gathering threat-interest groups together to share information more widely. Intelligence and information on any bad sources of information should be provided to various security elements for alerts to be raised. This would essentially allow users of such information to react according to their policy considerations. Using this source of intelligence would also mean that there would be less reliance on signatures and more on actual communication flows, which is a much lighter way of managing security.

Macaulay stated in conclusion that information, particularly information on malware, has to be derived from more than one source on the Internet and readily shared. He argued that it is only through information sharing and gathering from multiple sources that cyber-resilience can be built.

CYBER-SECURITY: IMPACT ON NATIONAL SECURITY AND BUSINESS OPERATIONS

Srijith Nair sharing his thoughts on India's national security during a syndicate discussion.

Srijith K. Nair spoke on the impact of cyber-attacks on India's national security and business operations. He also looked into the measures that could be taken to lessen the vulnerabilities of the information and communicatiaon technology systems (ICT).

India's interests in cyberspace has been under constant attack and one of the first few attacks which caught the attention of the Indian authorities was against the Bhabha Atomic Research Centre website. Hackers successfully managed to gain entry into the Research Centre's e-mail server which was also connected to the Centre's website. This allows the hackers to gain access to e-mails, lists of planned nuclear projects and files relating to India's nuclear research programme. This attack illustrates, in Nair's opinion, the extent and level of damage that future cyber-attacks could potentially inflict.

According to Nair, Symantec has stated in its 2010 State enterprise Security Study that 66 per cent of online Indian enterprises experienced some form of Internet-based attacks last year. Most of these are website defacement attacks which are political in nature and used as a method to further the propaganda of the relevant groups. However, these attacks affect the confidence of both customers and investors as they have the potential to create a negative perception of India's USD$47 billion information technology export industry.

Besides computer viruses and security breaches, India has also to deal with the presence of autonomy seeking splinter groups online. When it comes to dealing with such groups in cyberspace, the Indian government has relied on censorship. Nair asserted, however, that attempts to censor the Internet would not work unless it is done at the same stringent level as the Chinese government.

Nair pointed out that India is attempting to develop its own operating system due to fears that systems from other countries may not be secure. However, a high level of maturity is still needed to produce an operating system of calibre. The Indian Government has in June 2010 requested for Research In Motion (RIM), Skye and Google to make their data available only through legal demand. This is to ensure that elements such as terrorists do not use such means to communicate. This seems to be allowed through the recent Information Technology Amendment Act.

Despite the new cyber-security measures in place, it was commented that India still lacks a well-thought-out and cohesive cyber-strategy that covers all spectrum of problems. There is also a lack of investment in research and development. Moreover, while there has been a focus on combating cyber-crime, there are other problems on a national level that needed the attention of the government. Nair is of the opinion that India needs to work with likeminded countries and to develop frameworks to handle problems before they occur. He concluded that India has taken baby steps to improve its cyber-security but it is still a long way to go before the Indian cyber-space could be said to be truly secure.

SAFEGUARDING CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII) AGAINST CYBER-TERRORISM: CYBER-SECURITY MALAYSIA'S PERSPECTIVE

Zahri Yunos presenting on Malaysia's approach to cyber-security.

Zahri Yunos provided participants with an overview of the key aspects of Malaysia's critical national information infrastructure and the steps taken to safeguard it. The presentation began with an introduction to the operations of Cyber-Security Malaysia, a fully funded organization positioned as the national cyber-security specialist under the Ministry of Science, Technology and Innovation. Having started operations in 1997, Cyber-Security Malaysia maintains four areas of operation: (i) Cyber-Security Emergency Services; (ii) Security Quality Management Services; (iii) Training and Outreach; and (iv) Cyber-Security Research and Policy.

For Cyber-Security Malaysia, it subscribes to the definitions that cyber-crimes are "crimes committed in cyberspace" and cyber-terrorism is "the convergence of terrorism and cyberspace with such acts being politically motivated". Yunos noted that based on this set of definitions, attacks against non-essential infrastructure are categorized as a cyber-crime and not cyber-terrorism in Malaysia's context. With the current level of inter-dependency among various critical sectors, an attack on one sector would have adverse effects on other utility services. Due to the domino effect that a cyber-attack might have on the critical infrastructures and countries that depended on Web-based databases, for instance, terrorists are thus more interested in launching cyber-attacks than relying on traditional terrorist methods such as hostage taking, bombings and assassinations to assert their agenda.

As for Malaysia's initiatives to safeguard its information technology systems, Yunos highlighted that a national level security policy was developed with the objective of addressing the risk of the country's critical infrastructure. The security policy also aims to ensure that such infrastructures are protected at a level that commensurate with the risks involved. The country's critical sectors are divided into 10 key areas and they are: defence and security, banking and finance, transportation, health services, energy, information and communications, government, food, agriculture and water. The positive outcome of this initiative is that it brings different ministries and regulatory bodies that have a stake in cyber-security "under one roof"—a whole-of-government approach—with any resultant recommendations made escalated to the country's prime minister directly.

Yunos also added that this policy also spells out Malaysia's mitigation plan which is divided into eight key guiding frameworks and with each compartment headed by its respective ministries: effective governance, legislation and regulatory, cyber-security technology, culture of security and capacity building, research and development towards self reliance, compliance and enforcement, cyber-security emergency readiness and international cooperation.

In conclusion, Yunos underscored that increased cooperation, especially among the countries of the region, is necessary as today's terrorist(s) can do more harm with a keyboard than with a bomb.

DISCUSSION

In response to a question as to which category online stores such as eBay would fall into, a speaker replied that there are many sectors other than the financial sector that are prone to abuse and could be used for money laundering and terrorist financing purposes. However, these sectors are not regulated in the way that financial institutions are, with no provision made for them to understand and know their customers, and to report on suspicious transactions.

A participant sought to know whether Malaysia has any policies concerning terrorist websites hosted on ".my domains". In reply, a speaker mentioned that the Malaysian government does monitor such websites but at present it is still unclear as to what these websites aim to achieve. Finally, in answering a question on whether western militaries have any idea as to how many computers are infected by bots, a speaker noted that they are proactive and ready to take on radical steps to address the situation. That said, it was also highlighted from personal observations that given the level of sophistication that cyber-attacks take these days, even the civil service of nations such as Canada, and to a certain extent the United States, might find it challenging to resolve the problem promptly and entirely. Cyber-security is nonetheless an area or problem that affects everyone from the private to the public sector, and the local to the international community.

PANEL 5 – CYBER-THREAT MITIGATION STRATEGIES AND POLICY IMPLICATIONS

Foreign Policy & Cyber-security: From Domestic Imperative to Global

David Edelman presenting on the impact of cyber-security concerns on domestic security and foreign policy.

David Edelman's presentation focused on the complexities involved in the formulation of cyber-security policies and the need for an international consensus on cyberspace governance. The presentation commenced with a brief overview of the breath of issues which have been discussed in the conference, encompassing issues as diverse as the use of the Internet by terrorists to disseminate propaganda to the dangers that governments and businesses face with data security. As such, the need to create national security law for cyberspace that covers all relevant issues is enormously complex coupled with the need to build in intricate technical features that are difficult for the average policymaker to comprehend. Moreover, the issues involved often overlap into areas of criminality, counter-terrorism and, in some cases, traditional national security. Thus, this makes it difficult to identify the government arm that should be in charge of the problem, let alone what exact policy should be pursued. It was also mentioned that the greatest need in this field is "translation". He explained that many senior policymakers will not have in-depth technical knowledge of the field and "translation" is needed to bridge the gap between technical understanding and policymaking.

There are four lenses through which the problem of dealing with cyber-security matters could be viewed. The first involves national security implications. The United States and many other countries are increasingly dependent on the reliable and consistent functioning of technology for their daily operations. This dependency ironically forms the core of most national security problems especially since technological systems are extremely vulnerable to exploitation and those who seek to do damage have new vectors for doing so.

The second way to view the problem is through the lens of economic prosperity. A vast majority of the traffic on the Internet is economic in nature and millions of people are dependent on the Internet and cyberspace for their livelihood. The Internet with its open and inter-operable features was not built with security in mind. Policymakers, therefore, have to keep in mind the fact that they do not only have to create policy that promotes economic viability but also the promotion of security. It was also noted that the incentives for the public sector to adopt a more prudent approach and secure their own data against attacks might not be the same as the national security incentives to protect against foreign attacks.

The third lens through which to view this problem is the political perspective. The main issue here concerns the problem of competing regulatory framework and ownership. Very simply, which government arm is in charge and ultimately who gets to make the decisions on issues that affect not only the domestic but also the international sphere? Edelman stated matter-of-factly that every government industry now wants to play a part in cyber-security and this is increasingly so because it is the key to funding and the focus of the senior executive arm.

Finally, the problem can be viewed through the social lens. Edelman remarked that the public is generally unaware of impeding cyber-security threats. They do not use the latest operating systems and do not make sure that adequate firewalls are installed into their computers, which in his view, is a very real problem to address.

Edelman opined that from a policy perspective no single lens could give a complete representation of the complexity of cyberspace. When the entire society is at risk it really does require collaborative efforts between the private and public sector to resolve the problem together. It is also becoming evident that there is an expectation of reasonable behaviour in cyberspace and that instability in a country's technical network can result in instability in the international system. In conclusion, Edelman stressed that the goal in the next 10 years in policy circles is to develop and incentivize an international system whereby states see an intrinsic value in a productive and stable cyberspace. It would perhaps take a decade for consensus to be built around an international system like the cyberspace but it is absolutely necessary to ensure the best of what technology can offer remains safe and secure.

CRITICAL INFRASTRUCTURE INTERDEPENDENCY: METRICS-BASED ASSESSMENT AND POLICY INDICATIONS

Tyson Macaulay began his presentation on Critical Infrastructure Interdependency (CII) with a brief explanation of the reasons why inter-dependency metrics matter. This area is not well studied and whatever work that has been done so far has been inconclusive. The importance of CII lies in the fact that assessments are needed for business continuity, disaster recovery planning and managing enterprise risks.

Critical infrastructure (CI) also known as non-linearity or non-deterministic systems is extremely complex. Macaulay noted that in such a complex setting, a small change in the system can result in a massively different output. Using guesswork to try and estimate impacts that can be dramatically different can be problematic and that is why it is a necessity to move to a metrics-based system.

The CI sectors in Canada include the financial, telecommunication, energy, health, transportation, safety, food, water, manufacturing and government sectors. To assess inter-dependency, there is a need to understand the common resources or denominators that drives two related entities. Money, for instance, is a possible denominator as it is something that all CI sectors require to operate and will aim to generate. Additionally, as all infrastructures tend to exchange information at some point, another possible denominator is 'data'. According to Macaulay, when two metrics are present, correlation can be assessed. Correlation is the indication of two measures that move either in similar or opposite directions with the former indicating that a same variable is being measured.

CII is probably not widely considered in policy considerations because of its complexity. However, it is a topic that is always present in emergency-planning scenario. Macaulay cautioned one would risk missing out on other possible scenarios that could be generated should CII not be considered at all in the policy making process. In conclusion, it was highlighted that inter-dependency is measured against a time-scale as things do not stay the same and in fact changes the further it moves away from the impact event.

INFORMATION SECURITY STRATEGY IN JAPAN

Manabu Nabeshima sharing with participants how Japan has worked towards fostering public-private cooperation on information security management.

Manabu Nabeshima's presentation focused on Japan's cyber-security policies and in particular the building of public-private partnership on cyber-security matters. The goal of public-private partnership is to encourage all segments of society to take responsibility in the maintenance of cyber-security.

Nabeshima noted that Japan has thus far been successful in cultivating public-private partnership on environmental protection without the need to enforce a command-and-control type of legislation. Persuasion and understanding are the keys to successful public-private collaborations and Japan aims to replicate this partnership in its effort to secure the nation's information systems. It was articulated that the Japanese government has its limits in mandating commercial companies to take appropriate security measures; therefore the critical infrastructure industry has some responsibility to take to ensure the continuity of their systems.

There are 10 critical infrastructure sectors in Japan and they are namely: information communication, finance, airlines, railway, electric power, gas, government and administrative services, medical services, water and logistics. Each of these sectors has its own set of industry laws as the information system to be protected differs from sector-to-sector. To complement this and to standardize information protection across the board, Japan has adopted category-specific strategies such as the Action Plan on Information Security Measures for Critical Infrastructures (APCI).

Nabeshima elaborated that, like all policies, the APCI is designed to address issues at the governmental, critical infrastructure, business and individual levels. The APCI, it was added, is implemented by the National Information Security Centre (NISC) through five core programmes to ensure a total and holistic approach to information security. Firstly, the APCI complements the "Safety Standards and Guidelines" (SSG) which the NISC enforces to specify the information security measures to be taken by each critical infrastructure sector and areas that requires "priority security" (e.g. business continuity and prevention of information leak). Next, the APCI aims to build better collaboration on information security matters between the business community and public sector. This is done through the capacity of the Capability for Engineering of Protection, Technical Operation, Analysis and Response Council where the NISC takes on secretarial roles and actively supports information sharing among its members. Additionally, the NISC conducts common threat analysis and cross-sectoral exercises on a yearly basis. As such, the APCI serves auditory functions as well as facilitates emergency exercise. Finally, the NISC with the support of the critical infrastructure industry and through the APCI ensures that technological developments within the country support existing national efforts at protecting and conserving the environment.

In relation to businesses and individuals, Nabeshima highlighted that statistics compiled by Microsoft have shown that the infection rate for Japan is 0.3 per cent, which is considerably lower than the average world infection rate of 0.8 per cent. This implies that most Japanese are taking some measures to secure their information and networks. For instance, Nabeshima noted that more than 50 per cent of households in Japan have installed anti-virus software. As for businesses, the NISC and relevant ministries are introducing what is known as "Information Security Governance", which is the notion that a business should implement appropriate information security measures as a part of good corporate governance.

Nabeshima argued that as what is being protected belongs to the private sector, society therefore needs to take appropriate measures to secure their information network and systems. All in all, it was concluded that a whole-of-world approach and international collaboration is necessary to secure information and, essentially, the greater cyberspace.

DISCUSSION

A participant queried on the responsibility that countries should take especially when attacks could be traced to their infrastructure. In response, a speaker replied that at present, instead of holding states liable for acts committed in their domestic networks, the approach internationally is to treat such instances as cyber-crimes. Moreover, this is usually followed up with calls for greater cooperation among the various law-enforcement agencies. Countries have so far not been held responsible for cyber-attacks that have originated from their own networks. That said, however, individuals who are found to have broken criminal laws through their online activities are liable to prosecution and in some cases extradition.

In contrast to other countries, a participant commented that Japan holds a very remarkable record on information security management. This is especially since based on statistics, 80.2 per cent of Japanese households take some form of security precautions to secure their information system. It was asked if Japan's success at building public-private cooperation on information security matters is uniquely the work of culture. A speaker agreed and shared that most Japanese would have been taught the importance of, for instance, environmental and information protection, in school. This also attests to the importance of education and media in keeping the Japanese society abreast on national security priorities and needs.

PANEL 6
Roundtable Discussion: Policy Takeaways and The Way Forward

Speakers and participants engaged in active syndicate discussion.

The panel identified four key takeaways.

The first issue pertained to the establishment of a legal framework to deal with challenges that may arise. Noting that current responses to threats tend to be reactive—specifically tailored to the situation at hand—and also the different paces at which various stakeholders are responding to them, it was suggested that larger trends be identified by consolidating expertise on these issues. Following from this, these trends could be the basis for a legal framework to be built upon.

The second issue concerned the utility of developing a common lexicon for the discourse on cyber-security. On the one hand, proponents have argued that this would reduce conceptual ambiguity necessary for workable solutions to be devised. Moreover, it was also suggested that an operational definition of "cyberspace" could be premised on an information environment composed of connectivity, content and cognitive elements. On the other hand, it was pointed out that focus on the development of a consistent set of terms to this end should not be at the expense of developing high impact solutions.

The third issue related to calls for a holistic approach to tackle the challenges ahead. To this end, three areas for development were identified. The first was the need for robust technology to protect information assets, namely through the development of secure applications. The second was securing the expertise to develop and manage the systems in place which requires equipping staff with the relevant expertise to deal with the various challenges. The third was putting in place clear processes, namely policies, guidelines and standards. Moreover, with regards to priorities, it was stressed that technology was only an enabler while the problem solvers were people. Hence, investing in developing expertise and putting in place robust policies and processes should be the priority in dealing with cyber-attacks.

The fourth issue touched on the need to mediate expectations. While it was ideal to cultivate consensus and cooperation among various stakeholders to address ambitious objectives, the results tend to fall very short of the intended goals due to variations in levels of commitment and capabilities. Confidence building should, therefore, be concurrently complemented with a pragmatic focus on quick wins—the devising of simple policy fixes to address surmountable problems.

The key questions and comments from the audience were as follows.

On the question of the need for the development of an alternative system to mitigate the effects of a possible catastrophic cyber-attack and given society's current over-dependence on cyberspace, it was highlighted that the networked nature of cyberspace ironically makes the system resilient. While localized disruptions might occur in the event of a large-scale cyber-attack, a massive global outage remained highly unlikely.

On deterring perpetrators of cyber-attacks, it was suggested that a framework based on the concepts of attribution and deterrence could be developed. This approach was premised on making potential perpetrators believe the cost or consequences of inflicting an attack to be too high or unacceptable to them.

On future areas of research, it was noted that while many governments and businesses have shared their programmes and models on responding to cyber-threats, few studies exist that evaluated their effectiveness which would be useful for developing more robust solutions. The geostrategic implications of enhancing cyber-security via multilateral frameworks were also identified as another policy-relevant area of research.

Workshop Programme

Sunday, 11th July 2010

1700–1900hrs
Arrival of Invited Foreign Participants and Speakers
Venue : Marina Mandarin Hotel

1900–1945 hrs
Dinner Presentation
"**Cyber Security Within A Global Context**" by
Sheila Ronis,
Walsh College
Venue : Aquamarine (Level 4)
Attire : Smart Casual
(Long-sleeve shirt without tie)

1945–2100 hrs
Welcome Reception
Hosted by *Kumar Ramakrishna*,
Head, Centre of Excellence for National Security (CENS), RSIS, NTU and *Cung Vu*,
Defense Warning Office,
Global Futures Forum,
US Department of State
Venue : Aquamarine (Level 4)
Attire : Smart Casual
(Long-sleeve shirt without tie)

Monday, 12th July 2010

0800–0845hrs
Registration

0845–0900hrs
Welcome Remarks by
Cung Vu,
Defense Warning Office,
Global Futures Forum,
US Department of State and
Kumar Ramakrishna,
Head, Centre of Excellence for National Security (CENS),
RSIS, NTU
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)

0900–0915hrs
Welcome Address by
Peter Ho,
Permanent Secretary
(National Security and Intelligence Co-Ordination),
Ministry of Foreign Affairs

0915–0930hrs
Tea Break

0930–1030hrs
Keynote Speaker
"Securing Cyberspace: Priorities and Challenges" by
Ruth David,
President and CEO, ANSER

1045–1145hrs
Panel One – Overview of Cyber Threats, Criminal and Terrorist Online Activities to Date
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)
Chairperson:
Sheila Ronis,
Director, Walsh College
Speakers :
"Overview of Cyber Threats, Criminal and Terrorist Online Activities to Date" by
The Honourable John Grimes,
Former Assistant Secretary of Defense for Networks and Information Integration (ASD NII) / Department of Defense Chief Information Officer (CIO)

"Cyberspace – Taming the Wild West" by
John Savage,
Jefferson Science Fellow,
Office of Cyber Affairs
(US State Department) &
Brown University

“Evolution of Cyber Threats” by
David Aucsmith,
Senior Director,
Microsoft Institute for
Advanced Technology in
Governments

1145–1300hrs **Panel Two – Technological and Legal Tools**
Chairperson:
Sarah Womer,
Analyst, SAIC,
Open Source Exploitation
Speakers :
“Countering Terrorism on the Internet – Technological and Legal Tools”by
Alexander Lim,
Criminal Intelligence Analysis,
INTERPOL Liaison Office, Bangkok

“Controlling the Cyber Threat”
by *John Savage*,
Jefferson Science Fellow,
Office of Cyber Affairs
(US State Department) &
Brown University

“Cloud Computing Security –the Soft Spot” by
Anthony Lim,
Asia Pacific Director,
Application & Web Security,
IBM-Singapore

1300–1400hrs **Lunch**
Venue : Aquamarine (Level 4)

1400-1515hrs **Breakout Sessions**
(Syndicate Sessions to cover topics covered in panel 1 & 2)
Attire : Smart Casual
(Long-sleeve shirt without tie)
Group 1: Vanda Ballroom (Level 5)
Chairperson:
Susan Sim,
Strategic Nexus Consultancy

Group 2: Vanda 1 Meeting Rooms
(Level 6)
Chairperson:
Alexander Lim,
Criminal Intelligence Analysis,
INTERPOL Liaison Office, Bangkok

Group 3: Vanda 2 Meeting Rooms
(Level 6)
Chairperson:
Lori Lessner,
Analyst,
US Department of Defense

Group 4: Vanda 3 Meeting Rooms
(Level 6)
Chairperson:
Tyson Macaulay,
Security Liaison Officer,
Bell Canada, Canada

1515–1530hrs **Tea Break-Network Time**

1530-1600hrs **Syndicate Group Presentation**

1600–1800hrs **Panel Three- Implications For Homeland Security: (Country / Case Studies)**
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)
Chairperson:
Cung Vu,
Defense Warning Office,
Global Futures Forum,
US Department of State
Speakers:
“Online Influence, Indoctrination, and Recruitment“
by *Sarah Womer*,
Analyst, SAIC,
Open Source Exploitation

“Implications of the Evolving Internet“ by
Lori Lessner,
Analyst,
US Department of Defense

"Securing Philippine Cyberspace: Challenges and Issues" by
Nicolas Dy-Liacco Ojeda Jr.,
Chief of the Strategic and Special Studies, Armed Forces of the Philippines, The Philippines

1900-2100hrs **Wrap Up of Day 1** by
Cung Vu,
Defense Warning Office,
Global Futures Forum,
US Department of State
Venue : Tambuah Mas
Indonesian Restaurant
(Marina Square)
#02-04, 6 Raffles Boulevard
S(39594), Marina Square,
Marina Bay)
Attire : Smart Casual
(Long-sleeve shirt without tie)

Tuesday, 13th July 2010

0800-0845hrs **Registration**

0845–0900hrs **Review of Day One**
Kumar Ramakrishna,
Head, Centre of Excellence for National Security (CENS),
RSIS, NTU
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)

0900–1030hrs **Panel Four – Cyber Security from a "Real World" Perspective**
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)
Chairperson:
Anthony Lim,
Asia Pacific Director,
Application & Web Security,
IBM-Singapore

Speakers:
"Securing Banking Systems Against Financial Crimes and Terrorist Financing" by
Gunawan Husin,
RBS Global Banking and Markets,
Singapo*re*

"Hardening against modern malware ; Upstream intelligence and proactive security" by
Tyson Macaulay,
Security Liaison Officer,
Bell Canada, Canada

"Cyber Security: Impact on National Security and Business Operations" by
Srijith K. Nair,
Fellow of Cyber Strategy Studies
National Security Programme,
The Takshashila Institution, India

"Safeguarding Critical National Information Infrastructure (CNII) against Cyber Terrorism: Cybersecurity Malaysia's Persective" by
*Zahri Yuno*s,
Chief Operation Officer,
CyberSecurity Malaysia
(Ministry of Science, Technology & Innovation), Malaysia

Question & Answer

1030–1100hrs **Tea Break – Network Time**

1100–1230hrs **Breakout Sessions (Syndicate Sessions to cover topics covered in panel 3 & 4)**
Attire : Smart Casual
(Long-sleeve shirt without tie)
Group 1 : Vanda Ballroom (Level 5)
Chairperson:
Susan Sim,
Strategic Nexus Consultancy

Group 2 : Vanda 1 Meeting Rooms
(Level 6)
Chairperson:
Alexander Lim,
Criminal Intelligence Analysis,
INTERPOL Liaison Office, Bangkok

Group 3 : Vanda 2 Meeting Rooms
(Level 6)
Chairperson:
Lori Lessner,
Analyst,
US Department of Defense

Group 4 : Vanda 3 Meeting Rooms
(Level 6)
Chairperson:
Tyson Macaulay,
Security Liaison Officer,
Bell Canada, Canada

1230–1330hrs **Lunch – Network Time**
Venue : Ristorante Bologna
(Level 4)

1330–1400hrs **Syndicate Group Presentation Issues covered in Panel 3 and 4**
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)

1400–1600hrs **Panel Five - Cyber-threat mitigation strategies & Policy Implications: Towards a Whole-of-Society Approach to Cyber Security**
Venue : Vanda Ballroom (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)
Chairperson:
John Savage,
Jefferson Science Fellow,
Office of Cyber Affairs
(US State Department)
& Brown University

Speakers:
"Foreign Policy & Cybersecurity: From Domestic Imperative to Global" by
David Edelman,
Policy Advisor,
Office of Cyber Affairs, DOS

"Critical Infrastructure interdependency; metrics-based assessment and policy indications" by
Tyson Macaula,
Security Liaison Officer,
Bell Canada, Canada

"Information Security Strategy in Japan" by
Manabu Nabeshima,
Deputy Director,
National Information Security Center, Cabinet Secretariat, Japan

Question and Answer

1600-1620hrs **Tea Break – Network Time**

1620-1700hrs **Panel Six - Roundtable Discussion: Policy Takeaways and the Way Forward.**
Chairperson:
Ruth David,
President and CEO, ANSER
Selected speakers from previous panels.

1830-2100hrs **Closing Comments** by
Kumar Ramakrishna,
Head, Centre of Excellence for National Security (CENS),
RSIS, NTU
Venue : Peach Blossoms (Level 5)
Attire : Smart Casual
(Long-sleeve shirt without tie)

About GFF

What Is GFF?

The **Global Futures Forum (GFF)** is a multinational community initiated in 2005 that works at the open source level to identify and make sense of transnational threats. Its primary goal is to foster the development of enhanced insight and foresight among its membership through the exchange of different perspectives and through the utilization of collaborative research tools.

Who Is GFF?

GFF seeks to involve a diverse population of officials and subject-matter experts to stimulate cross-cultural and interdisciplinary thinking, and to challenge prevailing assumptions. GFF participants include government security officials, along with security-related experts from the academia, non-government organizations, and industry. More than 1,000 officials and experts from over 40 countries have taken part in GFF activities.

How Does GFF Work?

Face-to-Face Meetings
General Meetings: Washington in 11/2005, Prague in 12/2006, Vancouver in 4/2008, and Singapore in mid-2010.

Community of Interest Workshops: Small, topic-based meetings held regularly in various member countries.

GFF operates a password-protected website that is the repository of GFF production, including hundreds of readings and resources on relevant topics, member blogs, discussion forums, and wikis.

What are GFF Areas of Interest?

Current GFF communities of interest include Radicalization, Practice and Organization of Intelligence, Illicit Trafficking, Strategic Foresight and Warning, Terrorism and Counter-terrorism Studies, Proliferation, and Emerging and Disruptive Technologies.

For more information on GFF, please write to:
admin@globalfuturesforum.org

About CENS

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

Why CENS?

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

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

What Research Does CENS Do?

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

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

Radicalization Studies

- The multi-disciplinary study of the indicators and causes of violent radicalization, the promotion of community immunity to extremist ideas and best practices in individual rehabilitation. The assumption being that neutralizing violent radicalism presupposes individual and community resilience.

Social Resilience

- The systematic study of the sources of - and ways of promoting - the capacity of globalized, multicultural societies to hold together in the face of systemic shocks such as diseases and terrorist strikes.

Homeland Defence

- A broad domain encompassing risk perception, management and communication; and the study of best practices in societal engagement, dialogue and strategic communication in crises. The underlying theme is psychological resilience, as both a response and antidote to, societal stresses and perceptions of vulnerability.

Futures Studies

- The study of various theoretical and conceptual approaches to the systematic and rigorous study of emerging threats, as well as global trends and opportunities – on the assumption that Resilience also encompasses robust visions of the future.

How Does CENS Help Influence National Security Policy?

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

How Does CENS Help Raise Public Awareness of National Security Issues?

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

How Does CENS Keep Abreast of Cutting Edge National Security Research?

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

For More on CENS

Log on to **http://www.rsis.edu.sg** and follow the links to "Centre of Excellence for National Security".

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 the Senior Minister Professor S. Jayakumar.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS(NSIC) is Mr. Peter Ho, who is concurrently Head of Civil Service and Permanent Secretary for Foreign Affairs.

NSCS provides support to the ministerial-level Security Policy Review Committee (SPRC) and Senior official-level National Security Coordination Committee (NSCCom) and Intelligence Coordinating Committee (ICC). It organises and manages national security programmes, one example being the Asia-Pacific Programme for National Security Officers. NSCS also funds experimental, research or start-up projects that contribute to our national security.

NSCS is made up of two components: the National Security Coordination Centre (NSCC) and the Joint Counter-Terrorism Centre (JCTC). Each centre is headed by a director.

NSCC performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipating strategic threats. As a coordinating body, NSCC ensures that government agencies complement each other, and do not duplicate or perform competing tasks.

Visit the **www.nscs.gov.sg** for more information.

About the S. Rajaratnam School of International Studies (RSIS)

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

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

Graduate Training in International Affairs

RSIS offers an exacting graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (MSc) degrees in Strategic Studies, International Relations, International Political Economy and Asian Studies. Through partnerships with the University of Warwick and NTU's Nanyang Business School, **RSIS** also offers the RSIS-Warwick Double Masters Degrees (International Studies) as well as The Nanyang MBA (International Studies). The graduate teaching is distinguished by their focus on the Asia-Pacific region, the professional practice of international affairs and the cultivation of academic depth. Over 200 students, the majority from abroad, are enrolled with the School. A small and select Ph.D. programme caters to students whose interests match those of specific faculty members.

Research

Research at **RSIS** is conducted by five constituent Institutes and Centres: the Institute of Defence and Strategic Studies (IDSS), the International Centre for Political Violence and Terrorism Research (ICPVTR), the Centre of Excellence for National Security (CENS), the Centre for Non-Traditional Security (NTS) Studies, and the Temasek Foundation Centre for Trade & Negotiations (TFCTN). The focus of research is on issues relating to the security and stability of the Asia-Pacific region and their implications for Singapore and other countries in the region. The School has three professorships that bring distinguished scholars and practitioners to teach and do research at the School. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, and the NTUC Professorship in International Economic Relations.

International Collaboration

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

For more information on the School, **visit www.rsis.edu.sg**

PONDER THE IMPROBABLE

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

A Graduate School of Nanyang Technological University

Design by Oxygen Studio Designs

S. Rajaratnam School Of International Studies, Nanyang Technological University,
Block S4, Level B4, Nanyang Avenue, Singapore 639798
TEL 65-6790-6982 | FAX 65-6793-2991 | EMAIL wwwrsis@ntu.edu.sg | WEBSITE www.rsis.edu.sg