EFFECTIVE AND CREDIBLE CYBER DETERRENCE

27 – 28 MAY 2013, SINGAPORE

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

NSCS
NATIONAL SECURITY
COORDINATION SECRETARIAT

EFFECTIVE AND CREDIBLE CYBER DETERRENCE

REPORT ON THE WORKSHOP ORGANISED BY
THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (CENS)
AT THE S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES (RSIS),
NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

WITH THE SUPPORT OF
THE NATIONAL SECURITY COORDINATION SECRETARIAT (NSCS)
AT THE PRIME MINISTER'S OFFICE, SINGAPORE

27-28 MAY 2013
MARINA MANDARIN HOTEL
SINGAPORE

CONTENTS PAGE

Rapporteurs: Eliane Coates, Joseph Franco, Sulastri Osman, Nadica Pavlovska, Valerie Teo, Senol Yilmaz
Edited by: Caitriona H. Heinl

This report summarises 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 Rule. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

The workshop explored the fundamentals of developing the most effective and credible cyber deterrence strategies. Five panels and an interactive tabletop exercise were held from 27 to 28 May 2013 at the Marina Mandarin Hotel in Singapore.

The first panel focused on the development of counter-strategies against cyber threats to national security. Efficient cyber threat reduction with a focus on crafting national strategies to holistically and resourcefully mitigate risks, technical capabilities and political considerations in facing the challenges of cyber deterrence, and bridging the gap in law, policy and technology were discussed. The panel identified the increasing volume and sophistication of cyber attacks, interdependent systems, anonymity, difficulties of attribution, and balancing the need for freedom of information and security as the main cyber challenges to national security. Solutions provided included raising the costs of attacks for opponents while maximising our security benefits by agreeing on a common lexicon for cybersecurity, adopting risk-based approaches to prioritising threats and securing critical infrastructure, building national CERTs, gathering actionable intelligence, increasing attribution and offensive capabilities, increasing resilience, enhancing education and awareness, and fostering more public-private collaboration.

The second panel focused on credible cyber deterrence. Reducing cyber risks to critical infrastructure through the lens of the United States' National Institute of Standards and Technology's (NIST) collaborative approach, cyber power in the coming Cyber Westphalia Era, the building of systemic resilience, disruption, future deterrence, and kinetic cyber defence, with particular focus on Japan as a case study, were discussed. The collaborative process, which NIST is pursuing for the new United States Cybersecurity Framework, was discussed - it involves multi-stakeholder consultations with industry, government agencies, and academia to craft flexible and adaptable policies. Threat deterrence with focus on a "complex socio-technical" system so that deterrence could be provided through a combination of measures to promote resilience and actively disrupt "wicked actors" was discussed and attention drawn to the possible rise of cyberspace borders which could lead to a "Cyber Westphalian" age. The salient points of Japan's new cyber strategy were analysed and conclusion made that first strike deterrence is near to impossible – the key therefore is for states to demonstrate their kinetic potential to deter would-be aggressors.

The third panel focused on global cyber deterrence measures. ASEAN's cooperation on cybersecurity, the formulation of effective deterrence strategies in cyberspace, and global cyber deterrence challenges were discussed. An overview on ASEAN mechanisms, initiatives and plans to increase cybersecurity in its Member States, and the ASEAN Regional Forum (ARF) Statement on Cooperation in Fighting Cybercrime and Terrorist Misuse of Cyberspace was provided. Twelve factors falling into four broad categories (the fundamentals of deterrence, capabilities, legal and political factors, and wider factors) were outlined for consideration when defining a deterrence strategy. Finally, traditional deterrence theory and the challenges of applying it to cyber conflict were discussed. It was concluded that contrary to some beliefs, nuclear deterrence theory is not a unified, uncontested theory and therefore, although differences exist, complexities in cyber deterrence are not necessarily more complicated than nuclear deterrence strategy.

The fourth panel focused on international and regional governance for global cybersecurity. The role of INTERPOL and international coordination in the global fight against cybercrime, creating normative behaviour in cyberspace, and an International Telecommunication Union / International Multilateral Partnership Against Cyber Threats (ITU/IMPACT) case study on international cooperation to enhance cybersecurity readiness for nations were discussed. The INTERPOL Global Complex for Innovation (IGCI) which is due to be established in Singapore in 2014 in order to enhance cross-border police cooperation and its duo digital crime directorates which are due to serve as an international hub for cybercrime issues were discussed. Arguments were made for the promotion of more normative behaviour in cyberspace and for demystifying online threats by being clear about what they are and by responding at the different state, societal, sectoral, industry and individual levels. Finally, IMPACT objectives to assist member

countries develop their Computer Incident Response Teams (CIRTs), enhance public-private cooperation, and promote international cooperation to mitigate cyber threats were discussed.

The final panel focused on national level case examples and models of best practice. Singapore's cybersecurity strategies, China's Cybersecurity Review in 2012 from the perspective of China CERT (CNCERT), and new orientations in French cyber defence were discussed. It was concluded that one of the key elements in effectively dealing with cybersecurity threats is to undertake a collaborative approach involving citizens, the private sector and public administration. China's cybersecurity challenges in 2012 were outlined and elaboration provided on the different strategies that China has used in the past to deal with cyber attacks. Finally, the French White Paper on Defence and National Security, which was released at the end of April 2013, was discussed and an overview provided on French cyberspace defence and security with particular focus on civilian-military coordination and the usefulness of cyber reserves.

The final part of the workshop consisted of an interactive tabletop exercise organised and developed by the Infocomm Development Authority of Singapore (IDA) and the Centre of Excellence for National Security (CENS). Participants discussed two scenarios – cyber espionage and massive distributed denial-of-service (DDoS) attacks.

WELCOME REMARKS

Associate Professor Kumar Ramakrishna, Head of CENS, welcomed the participants on behalf of the Dean of RSIS, Ambassador Barry Desker, and the NSCS.

Ramakrishna noted that the workshop was organised at a very important time. Over the last ten months, countries in North America, the European Union, the Asia-Pacific and Russia had experienced a noticeable increase in cyber incidents. In addition to the financial sector, government agencies, military installations, financial houses, defence contractors, high tech companies, research firms and even academia have now been targeted as well. He brought attention to the speed at which cyber threats were constantly evolving, and provided examples of recent cyber attacks such as the Shamoon virus attack on oil suppliers, Red October and Gauss to underscore his points.

Ramakrishna outlined the aims and objectives of the workshop – to pool intellectual resources to suggest practical, innovative and creative solutions for tackling the increasingly significant and rapidly mutating global cyber threats. He said that the workshop's five panels and tabletop exercise (which was organised with the Infocomm Development Authority of Singapore (IDA)) were oriented towards finding relevant solutions.

He remarked that since cyber threats do not respect international boundaries, responses must be international. For this reason, guest speakers comprised representatives from Singapore, the region and across the international community. Furthermore, they formed a multi-stakeholder, interdisciplinary mix from the public and private sector, legal profession, diplomatic corps, industry and academia. Ultimately, the goal is to build an international "Community of Practice" comprising law enforcement, cyber experts, academics, the private sector, international organisations and NGOs to keep pace with the evolving cybersecurity landscape.

Finally, Ramakrishna noted that discussions would consider the feasibility of cyber deterrence, whether cyber deterrence is a good and workable idea, what it would entail, and how we can cooperate to make it work.

PANEL 1:

DEVELOPING COUNTER-STRATEGIES AGAINST CYBER THREATS TO NATIONAL SECURITY

Efficient Cyber Threat Reduction: Crafting National Strategies to Holistically and Resourcefully Mitigate Risks

Christopher Finan framed his presentation on efficient cyber threat reduction with a cost-benefit calculus toward the enemy – in other words, how to raise costs for the enemy while maximising our security benefits. He stressed the need for the cybersecurity community to come to terms with what cybersecurity means both technically and as a policy. He then laid out the following challenges: 1) agreeing to a common lexicon for cybersecurity; 2) a threat environment where capabilities are increasing incredibly fast with lone hackers, hacker collectives, nation states, organised criminals, and terrorists intending to use these capabilities; 3) asymmetry - for example, for every 10 million lines of defensive code, there are 125 lines of offensive code. This means USD$10 million is invested for every 125 lines of attack; 4) interdependent systems where disasters can have a domino effect; 5) the imperative of mitigating threats without restricting content by, for example, drafting a consumer Internet privacy bill of rights; 6) the imperative of promoting internet freedom; and 7) the imperative of a risk-based approach in protecting critical infrastructure.

There is a need to prioritise these risks due to limited government resources. The cybersecurity community does a good job in meeting challenges in horizontal multi-layered threats in the areas of physical security, data links, networks, transport, and application. However, policies are doing a poor job at addressing the multi-layered vertical space. The cybersecurity community needs to develop frameworks that align incentives between government and the private sector with the lightest government touch possible to optimise deterrence, therefore affecting the cost-benefit calculus of adversaries. Cybersecurity resiliency, barriers to entry, and costs to gain access should be raised. The benefits of successful intrusions should be reduced, and attribution, offensive capabilities and costs for conducting attacks should be increased.

Finan cautioned, however, against going too far so as to increase militarisation. He explained that it is important to stay attuned to both offensive and defensive technological developments. Strategies must balance security and privacy, security and regulation, the role of government and role of industry, and finally, resilience (or defence) and attribution (or offense) investments. Regulations should be minimised as much as possible and the private sector consulted in an ongoing public-private relationship. To conclude, the key to fostering public-private sector collaboration in cybersecurity is communication, transparency and a common lexicon.

The Challenges of Cyber Deterrence: Technical Capabilities and Political Considerations from International Experience

Ilias Chantzos explained that cyber is considered a Tier One threat by many countries and has been used as a means to launch significant intelligence collection attacks and even sabotage. He noted that attribution is difficult and that there is a dependence on technology,

which is rapidly evolving, as seen in the consistent increase of highly technical and specialised attacks by both state and non-state actors from 2009 to 2012. Most attacks are clearly criminal in nature and financially driven but an increasing number are targeted at foreign states.

He remarked that cyber deterrence dissuades the opponent from acting in a certain way for fear of the consequences. It requires preparedness, resilience, and a degree of retaliatory certainty, which is historically linked to offensive capability. Traditional deterrence concepts do not work well with cybersecurity. For example, in traditional security threats, there are declaratory postures, an ability to verify threats, demonstrable effects and effectiveness of attacks, first strike versus second strike calculations, offensive preferences and asymmetry. In cybersecurity however, there are no declarations, attacks are usually clandestine, there are no visible explosions, effectiveness is dependent on the opponent's resilience, attacks are almost always a second strike, it involves 'use-and-lose' technologies, and targeted attacks can be symmetric for offence and defence.

Chantzos suggested that effective cyber deterrence should be based on the following: Known unknowns, the identification of critical infrastructure and key government systems which must be defended, intelligence acquisition for situation awareness and early warning, preparedness, resilience-building in infrastructure and assets, capacity building to defend effectively (for example, national cyber defence planning as a part of the wider national security strategy), building national CERTs, plans for containment and mitigation of successful attacks, and cooperation with the private sector operating the infrastructure (by for example, building information sharing platforms).

An intelligence-centric approach is key to cybersecurity and has become the default posture but it is not enough. Actionable intelligence that is categorised, classified and prioritised to monitor and protect for real-time defence on multiple points, laws that allow access for defence, the acquisition and retention of technical skills, and processes which deliver effective incident responses and provide for decision-making can all help contain and mitigate attacks. In conclusion, Chantzos predicted that although the defensive-offensive debate will continue without a single correct answer, effective defence is likely to prove superior. The militarisation of some technologies is inevitable.

Developing Counter Strategies against Cyber Threats to National Security: Bridging the Gap in Law, Policy and Technology

Allan S. Cabanlong explained that the Philippine government is currently working on a Cyber Safe Government Network and Information Systems project. It is also crafting a policy on the Periodic Vulnerability Assessment of the Government's ICT Network and Systems.

He noted that public-private sector cooperation on cybersecurity issues is insufficient, that there is a lack of technology, and reactions to the Cybercrime Prevention Act of 2012 have been strong. On 11 May 2013, 30 government websites were subjected to DDoS attacks from Taiwan. IP addresses were traced to Taiwan but it could not be determined who the attackers were and/or if they were state-sponsored. Furthermore, government websites were hacked 1,353 times between 2003 and 2013. Most of these incidents coincided with the Philippine-China tensions, the Sulu-Sabah incursions and the disagreement with Taiwan. Attribution is very difficult and presents a dilemma of anonymity and traceability. Furthermore, the internet has no standard provisions for tracking or tracing and no laws to prohibit anonymity.

Cabanlong noted that immediate technical solutions include centralised hosting behind a fortified perimeter on uniform certified hosting platforms for custom content from agencies, a centralised web hosting facility for government websites, a common web platform, awareness campaigns, clear mandating, and

establishing Department of Science and Technology-Information and Communications Technology Office Government Computer Emergency Response Team (DOST-ICTO G/CERT). Near term requirements include accelerating rationalisation of DOST-ICTO to establish the institutional Chief Information Officer for the Government, institutionalisation of ICT policies for government, expansion of critical DOS-ICTO facilities (particularly key public infrastructure), and officially defining critical infrastructure. Medium term requirements include operationalising the Cybercrime Investigation and Coordination Council, developing and institutionalising the National Cybersecurity Plan, amending the Cybercrime Prevention Act, and establishing CERTs for all sectors.

In conclusion, he noted that the Philippines has to implement the National Cyber Security Strategy, strengthen international cooperation, lift the Temporary Restraining Order on the Cybercrime Prevention Act of 2012, and encourage public-private sector partnerships for combating cybersecurity threats. He noted that users are the weakest link in Philippine cybersecurity and although there is legislation, technology is inadequate. He concluded therefore that there is a need to bridge the gaps between legislation, policy and technology.

Discussion

The following points were made during the discussion.

A participant asked about the amount of effort being placed into profiling attacks so that the origins of attacks can be traced. A speaker responded that most attacks are intended to be clandestine so in principle there would not be a "big bang" – this is why Stuxnet was such a game-changer. There are however a number of incidents that are suggesting that it is not an inconceivable future outcome. Intelligence is being used to profile and track attacks. In the private sector however, technology companies are only tracking and profiling the means and methods of the attacks as these companies are not intelligence services and do not have the legal powers to profile and track attacks. There is a place for very overt campaigns but the current state of play is still very much clandestine. However, it may not stay that way forever.

A participant then asked about the certainty of cyber attacks since some uncertainty was also part of the deterrence dynamic in traditional nuclear security theory. A speaker responded that there is no MAD (Mutually Assured Destruction) equivalent for cybersecurity. Cases have demonstrated that cyber attacks can escalate to traditional security attacks but there is a need for a minimum demonstrable effect – to reach this level, there needs to be an ability to cause actual and significant disruption.

A participant asked about approaches to counter insider rogue agents. A speaker explained that insider threat is the most nefarious and historically it is very difficult to counter. Multi-layered defence, resilience, user access and authentication processes, and vetting of employees are part of raising costs for an adversary - every policy needs to address this issue. It seems that external attackers are by far the most prevalent. Furthermore, it is not about solely protecting the hardware – there must be protection against third parties, insiders and internal users' honest mistakes. Identities, authorisations, and physical security are each key points. However, security measures should also be in place to prevent users from making mistakes. Finally, internal user education and training is essential.

A participant asked how developing countries could develop cybersecurity policy. A speaker noted that a database is necessary to help prioritise risks and leverage market incentives to promote better cybersecurity. Developing countries have more potential for public-private cooperation since governments are involved in development from the beginning. There is more scope for creating frameworks where public and private sectors can cooperate effectively as they are still beginning to build institutions. However, they must strike a balance so that they maintain a light touch. Cybersecurity should be developed first before deterrence - build the wall first before worrying about who is attacking the wall. Start with a risk-based policy (for instance, what is the risk environment?) and determine how risks should be prioritised. Developing countries have the advantage of learning from others' mistakes and starting from scratch.

PANEL 2:

DEVELOPING CREDIBLE CYBER DETERRENCE

Reducing Cyber Risks to the Critical Infrastructure: NIST's Collaborative Approach

Timothy Grance first discussed the mandate of the United States National Institute of Standards and Technology (NIST) as laid out in Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*. The NIST was tasked to lead the creation of a Cybersecurity Framework that would enhance the resilience of critical infrastructure in the United States. The initiative was largely a response to the recognition that cybersecurity poses one of the most serious national security challenges that the U.S. must confront. For NIST to take the lead role was a natural progression since its mission is that of a "federal technology agency". As a non-regulatory agency, it has a solid reputation for being unbiased and technology-neutral. This allows NIST to focus on promoting innovation and industrial cooperation.

The multidimensional nature of cybersecurity threats and responses require strong links between key cybersecurity policy stakeholders such as industry players, government agencies and academia, which NIST promotes. For NIST, the creation of the Cybersecurity Framework is founded on a "risk-based approach" as required by Executive Order 13636. Solutions must be flexible, adaptable, performance-based, and cost effective. Grance stressed that the framework would not impose new standards especially when existing security protocols are already in place. It was also stressed that as a non-regulatory agency, the NIST will make sure that the framework would not compromise intellectual property rights, privacy, and civil liberties.

The linchpin of NIST's collaborative approach in creating the framework is a transparent process that seeks to solicit insights from the public. The framework development process is composed of iterative rounds of consultations - mostly through widely disseminated Requests for Information (RFIs). Grance pointed out that all responses to RFIs, whether short policy pieces, voluminous in-depth studies, or even marketing materials, are reviewed by NIST. NIST staff pore through the gathered inputs and organise the material into cybersecurity principles, practices, and gaps. All RFI responses are subsequently posted on the NIST Cybersecurity Framework website to further stimulate discussion within the stakeholder community.

To date, the draft framework has taken shape and the preliminary framework will be presented in September 2013. Grance expressed confidence that the collaborative approach will help incentivise participation. This process also provides a tacit approach for other regulatory agencies in the U.S. to reward good behaviour. Ultimately, the measure of the framework's success will come only if the private sector willingly "owns" the problem of critical infrastructure cybersecurity.

Cyber Power in the coming Cyber Westphalia era: Building Systemic Resilience, Disruption, and Future Deterrence

Chris C. Demchak defined cyberspace as a "substrate" that connects the wellbeing of societies. As a global "socio-technical system" it allows for the exchange of content and cognition. National power has become

"cybered" with tools of statecraft such as diplomacy, economics, and the military infused with information technology. Demchak argued that this has given rise to the spectre of "cybered conflict."

Cyber capabilities have endowed weak states and non-state actors with the ability to strike with scale, proximity and precision. Demchak highlighted the cost of these threats by quoting a U.S. Cyber Command official who remarked that expenses for cybersecurity were the greatest transfer of wealth in human history. Thus, global trends point to a move from the unsecure, open technologies and trust-based interactions that underpin the internet. She noted that there are four layers of surprise sources that can potentially stymie the interconnectivity of cyberspace: 1) normal surprise pertains to the routine complexity in the operation of any large organisation; 2) critical infrastructure surprise refers to the shocks that can be mitigated through national level resources; 3) bad actor surprise, which is brought about by small groups or individuals who threaten cyberspace-enabled systems through web access and 4) the wicked actors surprise - the most serious source of surprise since these actors have the ability to easily bypass cyber defences.

Drawing from lessons of complexity theory, large-scale technical systems research, and complex adaptive systems research, Demchak recommended two main approaches to accommodate surprises: resilience and disruption. Resilience should be used for responding to the first three sources of surprise. Specifically, resources should be focused on building sense-making capability and collective action mechanisms to detect attacks and promote sufficient "slack" capacity for systems. Wicked actors however, need to be confronted with more proactive disruption activities. While wicked actors only comprise 5 percent of potential threats, the disproportionate amount of damage they can cause justifies aggressive approaches. This entails "frustrating" wicked actors through law enforcement and technical means of "tailored disruption". Admittedly, the problem of attack attribution means that disruption is not scalable. Nonetheless, stakeholder willingness to use legitimate disruption is important to achieve deterrence.

To conclude, Demchak remarked that cyber deterrence is ultimately a product of cyber power. Deterrence is strongest when a nation state is able to act systematically to accommodate surprise. Military-style cyber commands should be expected as the "new normal." CERTs which focus largely on monitoring threats will yield to muscular CERTs, which have the capability to impose resilience and disruption. Continued changes in cyberspace, as a global socio-technical system, are expected to usher in a Cyber Westphalian system since building blocks for borders in cyberspace can only be expected to consolidate.

Kinetic Cyber Defence: The Case Study of Japan

Motohiro Tsuchiya described cyberspace as a new operational field in addition to the domains of land, sea, air, and space. Similar to physical domains, cyberspace has tangible components that can be subjected to attack. Tsuchiya was unconvinced that cyberspace is a "global commons". While information in cyberspace may appear intangible, it resides within an aggregation of interconnected devices such as individual computers, data storage centres, and submarine cables. He noted that even non-state actors are aware of the physical vulnerabilities of cyberspace as seen in a foiled plot to blow up a data centre in the United Kingdom. Tsuchiya remarked that the fusion of real space and cyberspace, as an operating environment and as a target, has prompted states to seriously consider expanding interagency approaches.

The Information Security Policy Council has released the *New Cybersecurity Strategy of Japan* - key points include: calls for cyberspace sanitation, the establishment of protocols for information sharing, promoting cybersecurity diplomacy and international norms, and the cultivation of "patriotic geeks." More importantly, the strategy seeks to redefine the cybersecurity role of the Japan Self-Defence Forces (JSDF). This involves the creation of a small hundred-man unit that would

be analogous to cyber commands established in other countries. Kinetic cyber defence involves the increased use of intelligence, surveillance, and reconnaissance (ISR).

Tsuchiya discussed the use of 'honey pots' to collect malware samples and ensnare cyber attackers. He also noted the development of tools such as the NICTER Atlas and DAEDELUS that provide policymakers with easy-to-use visualisation tools for monitoring incoming threats. While cyber threats may seem completely novel, he expressed optimism that existing principles based on international humanitarian law can be applicable in cyberspace. For instance, cyber operations can fall under Article 84 of the Self-Defence Force Act which covers "airspace intrusion." He noted that intrusion into cyberspace could be delineated by referring to "facility-based" bordering (for instance, protecting submarine cable landing sites). Another complementary approach he suggested is the use of existing discourse on territorial waters and concurrent rights of coastal states to allow innocent passage. For Tsuchiya, innocent passage is akin to the transit of a clean e-mail through a state's cyber infrastructure - a privilege accorded to individuals using the internet for legitimate purposes.

In conclusion, Tsuchiya stressed that it is possible to achieve deterrence. While stopping a first strike is nearly impossible, early detection can help stop a second wave. These measures should help position a state as a difficult target to attack.

Discussion

The following points were made during the discussion.

A participant asked whether states are falling into a trap of "over-territorialising" cyberspace in contrast to demands of the global economy. A speaker responded that cyberspace, specifically the internet, is characterised by either pairing or by subordinate relationships between users and infrastructure providers which require a degree of regulation. A participant then asked what the rationale behind applying international laws to cyberspace was since the diffused nature of jurisdiction could lead to "structural confusion" on who had the respective mandate to monitor, authorise and launch responses. A speaker responded that the problem of attack attribution is a perennial sticking point. Moreover, the difficulty in verifying cyber offensive capabilities can diminish the effectiveness of confidence-building measures through institutions such as the UN. Another point was raised regarding the apparent convergence of cyber commands and intelligence services in terms of their roles. The panel outlined the evolution of cyber commands, tracing their origins to signals and other covert units in intelligence agencies.

PANEL 3:

GLOBAL CYBER DETERRENCE MEASURES

ASEAN's Cooperation on Cybersecurity

Lu Choun Hian Leonard provided an overview of ASEAN's approach to cybersecurity. He began his presentation with an introduction to ASEAN mechanisms to increase cybersecurity. Four forums are used to discuss cyber-related security issues: 1) the ASEAN Ministerial Meeting on Transnational Crime; 2) the ASEAN Senior Officials Meeting on Transnational Crime; 3) the ASEAN Regional Forum (ARF); and 4) the ASEAN Telecommunications Regulators Council.

These fora have produced a number of initiatives to secure cyberspace. These initiatives include the ASEAN Declaration on Transnational Crime, the Plan of Action to Combat Transnational Crime, the Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crime, the ARF Statement on Cooperation in Fighting Cyber Attacks and Terrorist Misuse of Cyber Space, the ARF Statement on Cooperation in Ensuring Cybersecurity, and the Singapore Declaration to establish the ASEAN information infrastructure.

Lu then discussed the ASEAN ICT Masterplan 2015 (AIM2015), which was adopted in Kuala Lumpur in 2011. The two note-worthy components of the six-component Masterplan were: "People Engagement and Empowerment" and "Infrastructure Development". Under *People Engagement and Empowerment*, objectives include the promotion of secure transactions within ASEAN as well as reaching out to the public to increase awareness of cybersecurity related issues. Under *Infrastructure Development*, ASEAN aims to establish common minimum standards for network security, develop a network security "health screening" programme, develop best practice models for business continuity and disaster recovery for all sectors, establish the ASEAN Network Security Action Council to promote CERT cooperation and sharing of expertise, and share best practices on the protection of data and information infrastructure across ASEAN.

Regarding the countering of cybercrime, the ARF published a statement entitled Cooperation in Fighting Cybercrime and Terrorist Misuse of Cyber Space. Key points include: 1) promoting strategies to address threats emerging in this field consistent with international law and its basic principles; 2) promoting dialogue on confidence building and stability; 3) risk reduction measures to address the implications of ARF participants' use of ICT including exchange of views on the potential use of ICT in conflict; 4) encouraging and enhancing cooperation by creating a culture of cybersecurity; 5) developing an ARF work plan on security in the use of ICT focused on practical cooperation in confidence building measures; and 6) reviewing the possibility of elaborating common terms and definitions relevant to the use of ICT. To conclude, Lu discussed several projects between ASEAN and its internal and external partners.

Formulating Effective Deterrence Strategies for Cyber Space

John Bassett OBE discussed twelve factors for consideration when devising a deterrence strategy.

First, consensus is needed on who is to be deterred. Second, the deterring party must know what they are trying to deter from occurring. Bassett noted that in the nuclear context, deterrence failed to prevent adversaries from taking hostile actions. For example, despite being a nuclear power, the U.S. could not stop China from engaging in the Korean conflict. Similarly, the Falklands crisis erupted even though Britain was a nuclear power.

Third, awareness of credibility and how to build it is required - a party that is not credible will not be able to deter an opponent from taking undesired action. Fourth, in the cyber context, the question is whether cyber deterrence is technically feasible and whether the deterring party has the necessary technology to deter opponents. Fifth, the necessary technology must be disposable and usable in the real world. For instance, some technology might work in a laboratory but fail to operate as desired outside the laboratory. Sixth, apart from the technology, people with the right skills and knowledge are required. Furthermore, the numbers of people needed and the requisite type of skill set and knowledge must be known.

Seventh, it must be ensured that the law, both international and national, supports the deterrence strategy. Eighth, the strategy must be politically acceptable. In the nuclear context for example, deterrence was a sensitive issue and there was political opposition to the idea. Ninth, the strategy needs to be socially and economically viable. In the cyber context, security initiatives might easily infringe civil liberties and there could be suspicion of government-led surveillance of society. Tenth, wider factors must be considered. For example, it must be ascertained which partners (both domestic and international) are needed for this strategy. Furthermore, the strategy should be acceptable for audiences in political, economic, legal, and social terms. Eleventh, there must be an awareness of possible collateral damage and other unintended consequences, and twelfth, the strategy must be sustainable.

To conclude, Bassett noted that depending upon the context and operating environment, some factors are more important than others. If however, a number of factors are negative, the deterrence strategy could be doomed to fail.

Global Cyber Deterrence Challenges

Michael S. Chase discussed traditional deterrence theory and highlighted challenges in applying that theory to cyber conflict. He argued that in order to formulate a global cyber deterrence strategy, previous lessons from nuclear deterrence must be studied. Contrary to some beliefs, nuclear deterrence theory was not a unified, uncontested theory. Rather, many concepts were highly debated and not as clear as one might think. Therefore, the complexity of thinking about cyber deterrence is not necessarily more complicated than strategising about nuclear deterrence.

Chase quoted the following U.S. Department of Defense definition of deterrence: "The central idea of the Deterrence Operations Joint Operating Concept is to

decisively influence the adversary's decision-making calculus in order to prevent hostile actions against U.S. vital interests. This is the "end" or objective of joint operations designed to achieve deterrence.

Chase then suggested three kinds of deterrence: 1) deny the adversary's objectives. In the cyber context, this could be achieved by preventing network penetration (which would result in frustrating an opponent) or by strengthening the resilience of systems and networks so that cyber attacks do not cause persistent damage - possibly leading an opponent to realise that attacks are futile; 2) threat of punishment through a roughly proportionate cyber attack, through diplomatic and economic sanctions, or kinetic action. The deterring party's message is that it will inflict such heavy costs in response to an attack that the costs for an adversary will exceed any potential gains; and 3) encourage an adversary to refrain from taking action by communicating clearly that if the adversary refrains from acting, his cost-benefit calculation will yield a better result than if he/she had taken action.

Chase argued that in order to devise a good deterrence strategy, it must be determined to what extent traditional concepts apply. Also, there must be an awareness of who is to be deterred, from doing what, to whom, and how. In this regard, it could be useful to distinguish between cyberespionage and more damaging cyber attacks. Strategists need to bear three important factors in mind if they plan to deter by punishment. First, the context matters. Deterring strategic cyber attacks on critical infrastructure is different in a state of war than deterrence of a tactical cyber attack during peacetime. Second, a decision must be made in advance as to whether punishment will be limited to a cyber attack or whether it could be extended to a kinetic attack. Third, there is a communications challenge. In the nuclear context, opponents knew each other's capabilities and threats could be communicated convincingly. In the cyber context, capabilities are secret since making capabilities public could prompt defence measures by an opponent, thus rendering the cyber weapon useless.

Discussion

The following points were made during the discussion.

A participant asked whether CERTs have a deterrent effect. A speaker responded that it is better to have CERTs than not but at the same time they are only the most basic component of a whole strategy that needs to be in place to deter attacks. CERTs are very important - during the distributed denial of service attacks in Estonia, the Estonian government called CERT counterparts in other countries, which asked their Internet Service Providers (ISPs) to block traffic from the botnet to Estonia, helping alleviate damage from the attack.

When discussing cyber deterrence, the distinction between cyberespionage and more damaging cyber attacks might not be useful since Stuxnet for example, the most damaging known cyber weapon to date, was originally designed as a communication tool but was subsequently used to carry out an attack.

PANEL 4:

GLOBAL CYBERSECURITY: INTERNATIONAL AND REGIONAL GOVERNANCE

Cybercrime: International Coordination and the Role of INTERPOL

Madan M. Oberoi discussed the international coordination role of INTERPOL for cybercrime. INTERPOL has 190 member countries – it is the world's largest international police organisation and its main objective is to facilitate cross-border police cooperation in light of the advent of new age crimes like cybercrime which are multijurisdictional in nature.

Oberoi highlighted how police worldwide face an increasingly challenging operational landscape where criminals can take advantage of new technologies and anonymity proffered by the internet. In such an environment, law enforcement officers need real-time access to information across borders, and that is why the INTERPOL Global Complex for Innovation (IGCI) will be set up in Singapore in 2014. The innovation and research-based international coordination complex will be involved in training and capacity building, operational and investigation support, forging international partnerships, and development. The key aspect of IGCI, however, will be its duo digital crime directorates, which will serve as an international hub for cybercrime issues. The directorates will have the twin goal of executing cybercrime investigation requests and developing a cybercrime policy framework that could enhance cross-jurisdictional cooperation. The first directorate, the INTERPOL Digital Crime Centre, will provide a platform for the exchange of specialised police information, assist in cooperation on digital crime information, and support member countries by setting up digital forensic laboratories. The second directorate, Cyber Innovation and Outreach, will focus on the formulation of INTERPOL's global cybersecurity strategy through research and innovation.

Oberoi noted that international coordination is not without its issues. Cross-border cybercrime investigations require mutual legal assistance but existing mechanisms for such processes remain inadequate. The procedures for mutual legal assistance (MLA) requests, for instance, are time-consuming and there are disparities among member countries over what are considered crimes in cyberspace. Furthermore, informal cooperation between police agencies are usually only useful for preparations in the lead up to submission of formal MLA requests. He also noted that since MLA requests are largely bilateral in nature, they are neither broad-based nor widespread. Accordingly, Oberoi argued that there is a need to harmonise legal definitions and forensic standards to facilitate MLA requests across member countries. Multilateral conventions should also become more broad-based.

Oberoi noted that partnerships with multiple stakeholders such as the private sector, academia, and other international bodies need to be forged since law enforcement alone cannot keep up with rapidly evolving technologies. Furthermore, as the investigative capacity of any multijurisdictional investigation ultimately hinges on the capability and infrastructure of local law enforcement, local capabilities must also be built up. He further remarked that concerns over territorial sovereignty as well as individual privacy issues must be balanced. All in all, confidence and trust must be established in order to create the networking tools required for rapid information sharing. Oberoi concluded by arguing for the creation of a Global Clearing House for the expeditious exchange of subscriber information through a nodal agency.

Creating Normative Behaviour in Cyber Space

Heli Tiirmaa-Klaar advocated promoting more normative behaviour in cyberspace. She noted that international best practices and other similar policy fields lend themselves well to the development of norms in cyberspace. International institutions, for example, could offer ideas for good governance in the cyber domain.

Tiirmaa-Klaar explained that different kinds of security challenges and threats are faced in cyberspace and in order to properly respond to them, they must be first demystified. Such demystification is possible when there is intellectual clarity about what the challenges and threats are online and by responding to them at the different state, societal, sectoral, industry and individual levels. She suggested therefore that separate sets of normative behaviours, preventive measures, and even hard laws could be accordingly developed and tailored to these levels.

Tiirmaa-Klaar advised that it is useful to think about the response process as one that is about building trust in cyberspace, rather than one that is about establishing laws. She opined that all actors in the domain bear moral responsibility to preserve the benefits of cyberspace and that the same social responsibility existing offline should apply online. While there is no need to create new laws to replace existing ones, new soft norms are still needed. However, in light of the fact that 95% of cyberspace ultimately belongs to the private sector, it remains necessary to make an intellectual differentiation between norms for the private sector, for states, and for individual users. The private sector, for instance, could contribute to norms in cyberspace by participating in national cybersecurity coordination and governance systems, and crucially, by recognising the line of command in times of crises. States could contribute to normative behaviour in cyberspace through confidence building measures by having regular dialogues on cybersecurity and engaging in cyber diplomacy. Establishing contact points at different levels of government - at the decision-making, policy-making and technical levels - could further contribute to the process. Governments could also establish a set of cooperation obligations in crisis situations and exchange information regarding their national cybersecurity structures, their respective CERTs, and their responses to incidents in the private sector. They could also share threat information and set up early warning mechanisms.

However, Tiirmaa-Klaar noted that there are some challenges in the uneven level of national cybersecurity preparedness across regions and the differences in cyber governance structures. Furthermore, not all countries link cybersecurity with national security. Finally, since cyberspace has remained rule-free for so long, it would be difficult to play by new norms.

In conclusion, Tiirmaa-Klaar listed the five strategic priorities of the Cybersecurity Strategy of the European Union to: 1) achieve EU-wide cyber resilience; 2) reduce cybercrime; 3) develop cyber defence capabilities; 4) develop industrial and technological resources for cybersecurity; and 5) establish clear EU international cybersecurity policies. The principles of these policies are based on EU Member States' shared values on human rights, freedom of expression and rule of law. Finally, in order to ensure that internet architecture remains open and dynamic, a multistakeholder model of internet governance is favoured.

Enhancing Cybersecurity Readiness for Nations – International Cooperation: ITU-IMPACT Case Study

Philip Victor discussed the International Multilateral Partnership Against Cyber Threats' (IMPACT) work in assisting with enhancing national cybersecurity readiness of member countries of the International Telecommunication Union (ITU), a UN specialised agency. There are 145 countries involved in the ITU-IMPACT cybersecurity initiative, with the majority in Asia and Africa. Victor explained that IMPACT creates partnerships between academia, international organisations and think tanks, enhances public-private participation to build expertise, knowledge, skills, resources and experiences, and promotes international cooperation between states to mitigate cyber threats.

A key activity for IMPACT is to assist countries assess their existing cybersecurity postures in order to set up their national Computer Incident Response Teams (CIRT), and through capacity building programmes it helps member countries develop their CIRTs. The process includes gathering key stakeholders for a series of assessments and identifying gaps. Conducting cyber drills is another key IMPACT activity. The objective of cyber drills is to forge regional cooperation among different national CIRTs as well as to enhance communications and incident response capabilities. As CIRTs engage with one another through various scenario planning exercises, procedural processes can be refined within teams and better cooperation forged. Finally, IMPACT also provides training and skills development to help improve cybersecurity expertise within member countries and to develop child online protection national strategy frameworks.

In conclusion, global partnerships with those in industry, civil society, academia, and the private and public sectors are paramount for all IMPACT initiatives.

Discussion

The following points were made during the discussion.

A participant asked about cross-border data sharing and information exchange. A speaker noted that regarding requests to preserve cyber evidence (traffic logs for instance), there are standard procedures under the Budapest Convention. Furthermore, there are hotlines among G8 countries and beyond through which such requests could be made. Regarding concerns over privacy issues and balance with security considerations, countries have different security priorities and legal procedures. Even if a particular country has cyber legislation in place that allows for such sharing and exchange of information, it can decide to not do so should it feel that there would be no reciprocation from the other side. Therefore, there should be an institutionalised mechanism that could sufficiently address such issues from a wider global perspective.

PANEL 5:

NATIONAL LEVEL CASE EXAMPLES – MODELS OF BEST PRACTICE

Singapore's Cybersecurity Strategies

John Yong explained the role of the Infocomm Development Authority (IDA) of Singapore. He pointed out that the IDA has helped ICT become part of vibrant business systems, and mentioned that revenues from ICT have gradually increased - current revenue amounts to $82.42 billion out of which domestic revenue is $24.69 billion and export revenue is $58.73 billion. He also noted the increase in jobs created in this industry.

Yong then discussed the cybersecurity threat landscape. He sees cybersecurity threats from two perspectives – from policy and technical angles. For cyber threats, the policy may not be in place or the technical aspect of the threat may not be fully understood. The IDA closely monitors phishing emails - globally 1 in 500 emails are phishing emails. Occasionally, there is a drop in the number of phishing emails, which occurs when there is collaboration between ISPs and law enforcement agencies or through international collaboration. Regarding Singapore's cybersecurity strategy, he emphasised that the Government has taken a collaborative multi-agency approach. At strategic level, this is headed by the National Infocomm Security Committee, which comprises senior-level civil servants. One of the committee's goals was to create a "PPP" programme, which aims to strike a balance between the different interests of the public sector, the private sector and the peoples' interests. For this purpose, the Infocomm Security Awareness and outreach initiative was created through the cybersecurity awareness alliance to promote a greater adoption of essential security practices among users through education and training. The Cyber Watch Centre has also been established to closely monitor and provide pre-emptive alerts on a real-time basis in order to reduce the occurrence of security incidents. Finally, Yong discussed creating a secure and resilient Internet infrastructure. He pointed out that in 2011, a Code of Practice was issued that mandates ISPs to develop capabilities to manage emerging threats and participate in information sharing.

China's Cybersecurity Review in 2012: The Perspective of CNCERT

Zhu Tian discussed the role of China CERT (CNCERT) in China. It was established in 1999 and it is closely connected to the Government, the ISPs and the public. It has branches in 31 provinces across China and has successfully shaped a cross-network, cross-system, cross-regional technical support system for emergency response to public network security, sharing of information and national technical coordination. CNCERT services include monitoring, warning and notification, testing and evaluation, and incident(s) handling.

Zhu Tian then discussed on the cybersecurity landscape in China in 2012. During this period, China experienced a rapid evolution and integration of the internet; there are currently over 564 million users and about 420 million mobile net users. Although, the cybersecurity landscape remained stable, and there were no major incidents in 2012, there was still an increase in targeted attacks. She pointed out that the six main threats constantly faced by China included Trojans and botnets,

website security, phishing sites, mobile malware, vulnerabilities and DDoS attacks. The Government's response to these threats included security checks of the communication network and security checks of the ministries' websites. Furthermore, CNCERT in cooperation with the communications industry carried out a network security drill to strengthen collaboration in handling network security incidents jointly. The Government also urged ISPs to adopt effective techniques to clean up false IP addresses. Finally, there were six special campaigns to clean up mobile malware.

Zhu Tian discussed CNCERT's collaborative initiatives for dealing with online security threats such as ANVA, which was initiated by the Internet Society of China and operated by CNCERT to achieve a clean and safe online environment by fighting against malware and providing necessary technical support to the public. Members of ANVA include CERTs, ISPs, ICPs, domain registrars and network security vendors.

Regarding international cooperation on cross-border incidents, Tian explained that liaison mechanisms have been established between CNCERT and 91 CERTs from 51 different countries and regions. CNCERT has also signed or is signing cooperation agreements with 12 organisations. Cooperation includes providing assistance for cross-border network security incidents (in 2012, CNCERT assisted overseas organisations in 4,063 incidents).

New Orientations in French Cyber Defence

Patrice Tromparent noted that cyber attacks are listed under the main threats to national security identified under the recently released French White Paper on Defence and National Security. The White Paper delineates that cyber defence efforts are based on combined government/military cooperation.

Tromparent remarked that many ministries and administrative bodies deal with the cyber defence portfolio but there is a lack of coordination, which hinders opportunities to effectively address the challenges. In order to ensure coordination and coherence in the French administration, the French Network and Information Security Agency (ANSSI) was created in 2009. ANSSI has a central role in French cyber defence policy. It is the national authority for defence of information systems – therefore it not only has authority over the public sector but also over public and private operators of vital infrastructure in case of cyber crisis. It has the responsibility to monitor, detect, alert and react to possible network attacks, in particular to attacks on government networks. In the case of a major IT attack against the administration or an operator of vital infrastructure, ANSSI can enforce defence measures including the isolation of networks.

Some ministries also have a specific role: the Ministry for the Interior, is in charge of cybercrime, the Foreign Office, is responsible for coordinating diplomatic relationships, and the Ministry of Defence is responsible for defence of the information and communication systems. Tromparent then discussed the development of a "cyber reserve" under the French Ministry of Defence. This citizen reserve will be composed of actors from industry, the legal domain, politics, and the strategic domain and their main role is to promote cyber defence across the whole of society.

In conclusion, Tromparent discussed international cooperation on cyber defence issues. ANSSI, through the French CERT, has established relations with its counterparts. However, deeper engagement on these matters is very difficult since it involves discussing countries' vulnerabilities and core capacities.

Discussion

The following points were made during the discussion.

A participant asked about the merits of training cyber security professionals. A speaker responded that training is very important and for a small nation it is crucial since small countries must use all the resources they have at

their disposal. Furthermore, even cyber reserves could be used for training purposes. In Estonia for example, there is a voluntary cyber reserve force, which also trains younger people in industry or the private sector. Of course this cannot be applied to all countries.

A participant inquired if the ISP Code of Conduct in Singapore could be elaborated on further. A speaker replied that the ISP Code of Conduct was designed to encourage resiliency and security, and that many countries had similar regulations. Resiliency and security were complimentary, hence if the system was not resilient, security could not be robust and vice-versa.

WORKSHOP AGENDA

Monday 27 May 2013
Fundamentals of Effective Cyber Deterrence

0800 – 0900hrs **Registration**
Venue:
Vanda Ballroom Foyer (Level 5)

0900 – 0915hrs **RSIS Corporate Video + Welcome Remarks** by ***Kumar Ramakrishna****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

0915 – 1045hrs **Panel 1: Developing Counter-Strategies against Cyber Threats to National Security**
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

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

Speakers:
Efficient Cyber Threat Reduction: Crafting National Strategies to Holistically and Resourcefully Mitigate Risks by ***Christopher Finan,*** *Truman Project Fellow and Cyber Technology Development Consultant*

The Challenges of Cyber Deterrence: Technical Capabilities and Political Considerations from International Experience by ***Ilias Chantzos****, Senior Director, Symantec Government Affairs – EMEA and APJ*

Developing Counter Strategies against Cyber Threats to National Security: Bridging the Gap in Law, Policy and Technology by ***Allan S. Cabanlong,*** *Chief, Web Services and Cyber Security Division, Philippine National Police*

Q & A

1045 – 1100hrs **Tea Break**
Venue:
Vanda Ballroom Foyer (Level 5)

1100 – 1230hrs **Panel 2: Developing Credible Cyber Deterrence**
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

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

Speakers:
Reducing Cyber Risks to the Critical Infrastructure: NIST's Collaborative Approach by ***Timothy Grance****, Senior Computer Scientist, Information Technology Laboratory, National Institute of Standards and Technology (NIST)*

Cyber Power in the coming Cyber Westphalia era: Building Systemic Resilience, Disruption, and Future Deterrence by ***Chris C. Demchak,*** *Professor, Strategic Research Department and Co-Director, Center for Cyber Conflict Studies (C3S), U.S. Naval War College*

Kinetic Cyber Defense: The Case Study of Japan by ***Motohiro Tsuchiya,*** *Professor, Keio University*

Q & A

1230 – 1400hrs **Lunch**
Venue:
Pool Garden (Level 4)

1400 – 1525hrs **Panel 3: Global Cyber Deterrence Measures**
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

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

Speakers:
ASEAN's Cooperation on Cybersecurity by ***Lu Choun Hian Leonard,*** *Senior Officer, Security Cooperation Division, ASEAN Political Security Community, The ASEAN Secretariat*

Formulating Effective Deterrence Strategies for Cyber Space by ***John Bassett OBE,*** *Associate Fellow, Cybersecurity, Royal United Services Institute for Defence and Security Studies (RUSI)*

Global Cyber Deterrence Challenges by ***Michael S. Chase,*** *Associate Research Professor, Warfare Analysis and Research Department, Center for Naval Warfare Studies, U.S. Naval War College*

Q & A

1525 – 1545hrs **Tea Break**
Venue:
Vanda Ballroom Foyer (Level 5)

1545 – 1715hrs **Panel 4: International Norms & Confidence Building Measures**
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

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

Speakers:
Cybercrime: International Coordination and The Role of INTERPOL by ***Madan M. Oberoi,*** *Director of Cyber Innovation and Outreach Directorate, INTERPOL Global Complex for Innovation*

Creating Normative Behaviour in Cyber Space by ***Heli Tiirmaa-Klaar,*** *Cyber Security Policy Advisor, European External Action Service (EEAS)*

Enhancing Cyber Security Readiness for Nations – International Cooperation: ITU-IMPACT Case Study by ***Philip Victor,*** *Director, Policy and International Cooperation, IMPACT*

Q & A

1715hrs **End of Day 1**

1830 – 2100hrs **Workshop Dinner (by Invitation Only)**
Venue:
Aquamarine Restaurant (Level 4)

Tuesday, 28 May 2013

Global Cybersecurity – International & Regional Governance

0800 – 0900hrs **Registration**
Venue:
Vanda Ballroom Foyer (Level 5)

0900 – 1030hrs **Panel 5: National Level Case Examples – Models of Best Practice**
Venue:
Vanda Ballroom (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

Chairperson:
Yolanda Chin, *Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
Singapore's Cyber Security Strategies by ***John Yong,*** *Director, Infocomm Security & Assurance, Infocomm Development Authority of Singapore (IDA)*

China's Cyber Security Review in 2012: The Perspective of CNCERT by ***Zhu Tian,*** *Network Security Engineer, National Computer Network Emergency Response Technical Team/ Coordination Centre of China (CNCERT/CC)*

New Orientations in French Cyber Defense by ***Patrice Tromparent,*** *In Charge of Cyberdefense Issues, Defence Policy and Planning Department, Delegation for Strategic Affairs, French Ministry of Defence*

Q & A

1030 – 1245hrs **Table Top Exercise**
Venue:
Vanda Ballroom Foyer (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

1245 – 1400hrs **Lunch**
Venue:
Aquamarine Restaurant (Level 4)

1400 – 1620hrs **Table Top Exercise**
Venue:
Vanda Ballroom Foyer (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

1620– 1630hrs **Closing Remarks**
Venue:
Vanda Ballroom Foyer (Level 5)

Attire:
Smart Casual (Long-sleeved shirt without tie)

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

1630-1700hrs **Tea Break**
Venue:
Vanda Ballroom (Level 5)

1700hrs **End of Day 2**

1830 – 2100hrs **Dinner (by Invitation Only)**
Venue:
Peach Blossom Restaurant (Level 4)

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

John Bassett OBE
Associate Fellow
Cyber Security
Royal United Services Institute, London
61 Whitehall
London
SW1A 2ET
United Kingdom
Email: johnb@rusi.org

Allan S. Cabanlong
Police Chief Inspector
Web Services and Cyber Security Division
Head CyberSecurity ICTO
Philippine National Police
Camp Crame
Quezon City
Philippines
Email: llancop@yahoo.com

Ilias Chantzos
Senior Director
Government Affairs
Symantec Corporation
38 Medialaan Telekom Gardens
1800 Vilvoorde
Belgium
Email: ilias_chantzos@symantec.com

Michael S. Chase
Associate Professor
Center for Naval Warfare Studies
U.S. Naval War College
686 Cushing Road
Newport RI 02841
United States of America
Email: michael.chase@usnwc.edu

Chris C. Demchak
Professor
Strategic Research Department
U.S. Naval War College
686 Cushing Road
Newport R1 02842
United States of America
Email: chris.demchak@usnwc.edu

Christopher Finan
Fellow
Truman National Security Project
3422 Prospect St NW
Washington DC 20007
United States of America
Email: christopherfinan@hotmail.com

Timothy Grance
Senior Computer Scientist
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-8930
United States of America
Email: grance@nist.gov

Lu Choun Hian Leonard
Senior Officer
Security Cooperation Division
ASEAN Political Security Community (APSC) Department
ASEAN Secretariat
70A, Jl. Sisingamangaraja
Jakarta 12110
Indonesia
Email: leonard.lu@asean.org

Madan M. Oberoi
Director of Cyber Innovation and Outreach Directorate
INTERPOL Global Complex for Innovation (IGCI),
Singapore
7th Floor Delhi Police Headquarters
IP Estate
New Delhi 110002
Email: mmoberoi@yahoo.com

Heli Tiirmaa-Klaar
Cyber Security Policy Advisor
European External Action Service (EEAS)
9 Schuman Roundabout
Brussels
Belgium
Email: heli.tiirmaa-klaar@eeas.europa.eu

Patrice Tromparent
Directorate for Strategic Affairs
Defence Policy Department
French Ministry of Defence
14 rue Saint-Dominique
75700 Paris SP 07
France
Email: patrice.tromparent@intradef.gouv.fr

Motohiro Tsuchiya
Professor
Keio University
5322 Endo Fuisawa
Kanagawa 252-0882
Japan
Email: taiyo@sfc.keio.ac.jp

Philip Victor
Director for Policy and International Cooperation
International Multilateral Partnership Against Cyber Threats (IMPACT)
Jalan IMPACT
63000 Cyberjaya
Malaysia
Email: philip.victor@impact-alliance.org

John Yong
Director
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: john_yong@ida.gov.sg

Tian Zhu
Network Security Engineer
National Computer Network Emergency Response Technical Team
Coordination Center of China
No. 3 Jia Yumin Road, Chaoyang District
Beijing, 100029
People's Republic of China
Email: zhutian@cert.org.cn

CHAIRPERSONS

Damien D. Cheong
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isdcheong@ntu.edu.sg

Yolanda Chin
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: istlchin@ntu.edu.sg

Caitriona H. Heinl
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: ischeinl@ntu.edu.sg

Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: iskumar@ntu.edu.sg

Norman Vasu
Assistant Professor and Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isnvasu@ntu.edu.sg

LIST OF PARTICIPANTS

Mely Caballero Anthony
Associate Professor and Head
NTS Studies
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: ismcanthony@ntu.edu.sg

Benedict Chen
Analyst
Ministry of Defence (MINDEF)
Blk 303 Gombak Drive #01-52
Singapore 669645
Email: chee_siew_hong@starnet.gov.sg

Chiew Jingyi
Senior Engineer
National Security Engineering Centre
Defence Science & Technology Agency (DSTA)
1 Depot Road
Singapore 109679
Email: cjingyi@dsta.gov.sg

Colin Chiok
Assistant Director, Engagement and Training
National Maritime Sense-making Centre (NMSC)
National Maritime Security Singapore (NMSS)
AFPN 6504
103 Tanah Merah Coast Road #01-04
Singapore 498750
Email: colin_chiok@nmss.gov.sg

Chong Chia Siong Alan
Associate Professor
Military Studies Programme
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: iscschong@ntu.edu.sg

Choo Wei Liang Timothy
Senior Asst Director
Collection Branch
Singapore Prison Service (Headquarters)
407 Upper Changi Road North
Singapore 507658
Email: timothy_choo@pris.gov.sg

Elaine Ee
Senior Analyst
National Maritime Sense-making Centre (NMSC)
National Maritime Security Singapore (NMSS)
Command Post AFPN 6504
103 Tanah Merah Coast Road #01-33
Singapore 498750
Email: elaine_ee@nmss.gov.sg

Kannan Gnanasihamani
Senior Director
Technology Crime Unit (TCU)
Attorney-General's Chambers (AGC)
1 Upper Pickering Street
Singapore 058288
Email: kannan_g@agc.gov.sg

Cleo Haynal
Analyst
International Centre for Political Violence and Terrorism Research (ICPVTR)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: cleohaynal@gmail.com

Elena Ho
Admin Manager
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isewlho@ntu.edu.sg

Ho Lye Seng
Deputy Director
Ministry of Home Affairs (MHA)
28 Irrawaddy Road
Singapore 329560
Email: ho_lye_seng@mha.gov.sg

Ho Tze Ern Benjamin
Associate Research Fellow
Institute for Defence and Strategic Studies (IDSS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isteho@ntu.edu.sg

Hoh Wai Kiat
ICT Security Officer
Singapore Civil Defence Force (SCDF)
91 Ubi Avenue 4
Singapore 408827
Email: dickson_hoh@scdf.gov.sg

Yuki Honda
Digital Crime Officer
INTERPOL Digital Crime Centre (IDCC)
INTERPOL Global Complex for Innovation (IGCI)
IGCI Transition Support Office
HomeTeam Clubhouse
31 Ah Hood Road #03-19
Singapore 329979
Email: y.honda@interpol.int

How Jing Lin
Associate Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: how_jing_lin@ida.gov.sg

Rehan Hussin
Assistant Director
Analysis
National Maritime Sense-making Centre (NMSC)
National Maritime Security Singapore (NMSS)
AFPN 6504
103 Tanah Merah Coast Road #01-04
Singapore 498750
Email: rehan_hussin@spf.gov.sg

Domingo Molina Jr
Senior Assistant Director
Joint Training Centre (JTC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: domingo_molina_jr@mha.gov.sg

Kalaivanan
Deputy Superintendent
Singapore Prison Service (PRIS)
21 Admiralty West Prison
Admiralty Road West
Sembawang
Singapore 757698
Email: kalaivanan_visvalingam@pris.gov.sg

Martin Khoo
Deputy Director
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: martin_khoo@ida.gov.sg

Kong Wei-Chang
Associate Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: kong_wei_chang@ida.gov.sg

Lee Liang Chye
Head Technical Support
Singapore Police Force (SPF)
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: lee_liang_chye@spf.gov.sg

Eric Lim
Analyst
Ministry of Home Affairs (MHA)
New Phoenix Park
30 Irrawaddy Road
Singapore 329561
Email: mha_training_command@mha.gov.sg

Lim Wuei Kang
Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: lim_wuei_kang@ida.gov.sg

Lim Yan Chiang Jimmy
Senior Executive
Civil Service College (CSC)
31 North Buona Vista Road
Singapore 275983
Email: jimmy_lim@cscollege.gov.sg

Ling Kok Yong
Director
Singapore Civil Defence Force (SCDF)
91 Ubi Avenue 4
Singapore 408827
Email: ling_kok_yong@scdf.gov.sg

Loo Chee Tat Raymond
Group Leader
Ministry of Defence (MINDEF)
Blk 303 Gombak Drive #01-52
Singapore 669645
Email: chee_siew_hong@starnet.gov.sg

Low Fook Chuen
Senior Assistant Executive
Joint Training Centre (JTC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: low_fook_chuen@mha.gov.sg

Nur Azlin Mohamed Yasin
Associate Research Fellow
International Centre for Political Violence and Terrorism Research (ICPVTR)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isnurazlin@ntu.edu.sg

Neo Loo Seng
Senior Research Analyst
Home Team Behavioural Sciences Centre (HTBSC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: neo_loo_seng@mha.gov.sg

Ng Lup Houh
Deputy Director
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: ng_lup_houh@ida.gov.sg

Thomas Ng E Siong
Deputy Director
Cyber Security Response
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: ng_e_siong@ida,gov.sg

Chris Ng Wee Kiat
Senior Engineer
National Security Engineering Centre
Defence Science & Technology Agency (DSTA)
1 Depot Road
Singapore 109679
Email: nweekiat@dsta.gov.sg

Teddy Ong
Assistant Director
Ministry of Home Affairs (MHA)
New Phoenix Park
30 Irrawaddy Road
Singapore 329561
Email: teddy_ong@mha.gov.sg

James Pang
Assistant Director
Digital Crime Investigative Support
INTERPOL Digital Crime Centre (IDCC)
INTERPOL Global Complex for Innovation (IGCI)
IGCI Transition Support Office
HomeTeam Clubhouse
31 Ah Hood Road #03-19
Singapore 329979
Email: j.pang@interpol.int

Nur Azha Putra
Research Associate
Energy Studies Institute (ESI)
29 Heng Mui Keng Terrace
Block A, #10-01
Singapore 119620
Email: azha@nus.edu.sg

Benjamin Quek
Senior Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: benjamin_quek@ida.gov.sg

Jane Quek
Psychologist
Home Team Behavioural Sciences Centre (HTBSC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: quek_jane@mha.gov.sg

Fadzil Abdul Rahman
Assistant Director
Centre for Protective Security Studies (CPSS)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: fadzil_abd_rahman@mha.gov.sg

Md Faizal Abdul Rahman
Deputy Director
International Engagement & Partnerships
Ministry of Home Affairs (MHA)
New Phoenix Park
30 Irrawaddy Road
Singapore 329561
Email: md_faizal_abdul_rahman@mha.gov.sg

Roy Rimington
Senior Consultant
Civil Service College (CSC)
31 North Buona Vista Road
Singapore 275983
Email: excelpursuit@gmail.com

Thiyagarajan RRS
Assistant Director
Civil Emergency
Joint Training Centre (JTC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: thiyagarajan_rrs@mha.gov.sg

Eddy Sahran
Assistant Director
Stimulation Training
Joint Training Centre (JTC)
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: eddy_sahran@mha.gov.sg

Nur Irfani Binte Saripi
Associate Research Fellow
International Centre for Political Violence and Terrorism Research (ICPVTR)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: isnurirfani@ntu.edu.sg

Felina Silva
Senior Executive
Management Development
Civil Service College (CSC)
31 North Buona Vista Road
Singapore 275983
Email: felina_wenslaus_silva@cscollege.gov.sg

Sim Chun Yong
Assistant Director, Research
National Maritime Security System (NMSS)
103 Tanah Merah Coast Road #01-03
Singapore 498750
Email: sim_chun_yong@ica.gov.sg

Sim Kwang Xiong
Policy Officer
Ministry of Defence (MINDEF)
Blk 303 Gombak Drive #01-52
Singapore 669645
Email: sim_kwang_xiong@mindef.gov.sg

Sim Li Guek
Senior Assistant Executive
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: sim_li_guek@mha.gov.sg

Clifton Soh
Incident Responder
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: clifton_soh@ida.gov.sg

Eu-Gene Soh
Head Strategic Project Management
INTERPOL Global Complex for Innovation (IGCI)
IGCI Transition Support Office
HomeTeam Clubhouse
31 Ah Hood Road #03-19
Singapore 329979
Email: e.soh@interpol.int

Dalton Tan
Director, South East Asia
FireEye
9 Battery Road
11/F Straits Trading Building
Singapore 049910
Email: dalton.tan@fireeye.com

Tan Eng Keong
Senior Assistant Director
Singapore Prison Service (PRIS)
Operations Management Branch
407 Upper Changi Road North
Singapore 507658
Email: tan_eng_keong@pris.gov.sg

Geraldine Tan
Deputy Director
Technology & Operations
Ministry of Home Affairs (MHA)
28 Irrawaddy Road
Singapore 329560
Email: geraldine_tan@mha.gov.sg

Hannah Tan
Assistant Director
National Security Coordination Secretariat (NSCS)
55 Newton Road #15-01
Revenue House
Singapore 307987
Email: hannah_tan@nscs.gov.sg

Tan Sai Lan
Manager
Maritime and Port Authority of Singapore (MPA)
460 Alexandra Road
PSA Building #19-00
Singapore 119963
Email: sai_lan_tan@mpa.gov.sg

Tan Sherwayn
Ministry of Defence (MINDEF)
Blk 303 Gombak Drive #01-52
Singapore 669645
Email: tan_sherwayn@mindef.gov.sg

Tan Tiong
Manager
Maritime and Port Authority of Singapore (MPA)
460 Alexandra Road
PSA Building #19-00
Singapore 119963
Email: tiong_tan@mpa.gov.sg

Victor Tan
Senior Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: victor_es_tan@ida.gov.sg

Tan Wei Chong
Branch Head
Ministry of Defence (MINDEF)
308 Gombak Drive #05-01
Singapore 669646
Email: tan_wei_chong@mindef.gov.sg

Teo Di Kai
Staff Officer
Ministry of Defence (MINDEF)
Blk 303 Gombak Drive #01-52
Singapore 669645
Email: teo_di_kai@starnet.gov.sg

Grace Teo Pei Pei
SO IT Security Mgt
Singapore Civil Defence Force (SCDF)
91 Ubi Avenue 4
Singapore 408827
Email: grace_teo@scdf.gov.sg

Thng E-shen
Analyst
Ministry of Home Affairs (MHA)
New Phoenix Park
30 Irrawaddy Road
Singapore 329561

Nelson Jay Timbang
Philippine Navy International Liaison Officer
Information Fusion Centre, RSN
103 Tanah Merah Coast Road #01-02
Singapore 498750
Email: timbang.nelson13494@navy.mil.ph

Alex Toh
Associate Consultant
Infocomm Development Authority (IDA) of Singapore
10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438
Email: alex_toh@ida.gov.sg

Pascal Vennesson
Professor
Military Studies Programme
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University
Block S4 Level B4
Nanyang Avenue
Singapore 639798
Email: ispvennesson@ntu.edu.sg

Angel Zaratan Viliran
Philippine Navy International Liaison Officer
Information Fusion Centre, RSN
103 Tanah Merah Coast Road #01-02
Singapore 498750
Email: angel.viliran@coastguard.gov.ph

Stella Wee
Analyst
Ministry of Home Affairs (MHA)
New Phoenix Park
30 Irrawaddy Road
Singapore 329561

Wong Jin Yong
Senior Manager
Maritime and Port Authority of Singapore (MPA)
460 Alexandra Road
PSA Building #19-00
Singapore 119963
Email: jin_yong_wong@mpa.gov.sg

Wong Ko Foon
Assistant Director
Strategic Planning
Home Team Academy (HTA)
501 Old Choa Chu Kang Road
Singapore 698928
Email: wong_ko_foon@mha.gov.sg

Yau Chen Hui
Head ICT Security Management
Singapore Police Force (SPF)
New Phoenix Park
28 Irrawaddy Road
Singapore 329560
Email: yau_chen_hui@spf.gov.sg

Yeo Jian Cong, Aiden
Assistant Director
Information Management
National Maritime Security System (NMSS)
103 Tanah Merah Coast Road #01-30
Singapore 498750
Email: aiden_yeo@customs.gov.sg

Vanessa Yew
Senior Executive
International Engagement & Partnerships
Ministry of Home Affairs (MHA)
28 Irrawaddy Road
Singapore 329560
Email: vanessa_yew@mha.gov.sg

Victor Yiu
Assistant Manager
Civil Service College (CSC)
31 North Buona Vista Road
Singapore 275983
Email: victor_yiu@cscollege.gov.sg

ABOUT CENS

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

Why CENS?

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

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

What research does CENS do?

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

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

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

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

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

HOW DOES CENS HELP INFLUENCE NATIONAL SECURITY POLICY?

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

HOW DOES CENS HELP RAISE PUBLIC AWARENESS OF NATIONAL SECURITY ISSUES?

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

HOW DOES CENS KEEP ABREAST OF CUTTING EDGE NATIONAL SECURITY RESEARCH?

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

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

ABOUT RSIS

The **S. Rajaratnam School of International Studies** (**RSIS**) was officially inaugurated on 1 January 2007. Before that, it was known as the Institute of Defence and Strategic Studies (IDSS), which was established ten years earlier on 30 July 1996. Like its predecessor, **RSIS** was established as an autonomous entity within Nanyang Technological University (NTU). **RSIS**' aim is to be a leading research institution and professional graduate school 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, international political economy, diplomacy and international relations
- Collaborate with like-minded schools of international affairs to form a global network of excellence

GRADUATE EDUCATION IN INTERNATIONAL AFFAIRS

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The teaching programme consists of the Master of Science (M.Sc.) 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 NTU-Warwick Double Masters Programme as well as The Nanyang MBA (International Studies). Teaching at RSIS is distinguished by its focus on the Asia Pacific region, the professional practice of international affairs and the cultivation of academic depth. Over 230 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 six 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; the Temasek Foundation Centre for Trade & Negotiations (TFCTN) and the Centre for Multilateralism Studies (CMS). 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 four endowed 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, the NTUC Professorship in International Economic Relations and the Bakrie Professorship in Southeast Asia Policy.

INTERNATIONAL COLLABORATION

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

For more information about **RSIS**, visit http://www.rsis.edu.sg

ABOUT NSCS

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

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

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

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

For more information about **NSCS**, visit http://www.nscs.gov.sg/

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