APPSNO

7th ASIA-PACIFIC PROGRAMME

FOR SENIOR NATIONAL SECURITY OFFICERS (APPSNO)

8 - 12 APRIL 2013, SINGAPORE

Narrowing the Theory-Practice Gap

PONDER THE IMPROBABLE

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

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

7th Asia-Pacific Programme for Senior National Security Officers (APPSNO)

REPORT ON THE CONFERENCE 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

8 – 12 APRIL 2013
THE SENTOSA, A BEAUFORT HOTEL, SINGAPORE

CONTENTS PAGE

Rapporteurs: Damien D. Cheong, Yolanda Chin, Eliane Coates, Joseph Franco, Nadica Pavlovska, Valerie Teo, Jennifer Yang Hui, Yeap Su Yin

Edited by: Sulastri Osman

This report summarises the proceedings of the conference as interpreted by 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.

BACKGROUND AND AIMS OF THE CONFERENCE

National security is today a complex domain, encompassing matters ranging from the challenges of homeland security management, to designing coping strategies for a wide variety of traditional and non-traditional threats. National security, especially in a rapidly changing and complex environment, remains a key concern for countries worldwide.

In line with this, and with the aim of promoting a multi-agency and networked government approach as an important response to today's complex and uncertain security milieu, the Centre of Excellence for National Security (CENS), a research unit of the S. Rajaratnam School of International Studies (RSIS) with the support of the National Security Coordination Secretariat (NSCS), part of Singapore's Prime Minister's Office, has organised the 7th Asia-Pacific Programme for Senior National Security Officers (APPSNO). APPSNO is targeted at senior government officials from the Asia-Pacific and beyond with responsibilities for national security matters. It is hoped that APPSNO would become an important tool for promoting the analytical frameworks, mindsets and skills needed for effective national security management.

APPSNO is driven by two primary objectives:

1. **Enhance exposure to global best practices in national security**
   Participants were given the opportunity to learn about the trends and global best practices in national security issues through lectures and informal discussions. Prominent speakers this year were invited to speak on topics related to national risk assessment and management, strategic and crisis communication, cybersecurity, and countering violent extremism and radicalisation. The small-group interactive discussion format enabled participants to share ideas, anecdotes and experiences that were of broad professional interest.

2. **Facilitate an international network of national security experts and practitioners**
   APPSNO provided the platform for participants to network with global national security experts as well as develop stronger relationships with their regional counterparts. Interaction were facilitated through field visits, educational and study tours and social activities.

EXECUTIVE SUMMARY

OPENING REMARKS

Ambassador Barry Desker, Dean, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU)

In his opening remarks, Ambassador Barry Desker welcomed participants to the 7th Asia-Pacific Programme for Senior National Security Officers (APPSNO). In line with the APPSNO 2013 theme of "Narrowing the Theory-Practice Gap", Ambassador Desker encouraged participants to discuss practical ways in which policy practitioners could deal with complex national security challenges through strategic partnership with academic research. In this regard APPSNO was well-placed to bridge the engagement between academia and policymakers.

OPENING ADDRESS

Mr. Teo Chee Hean, Deputy Prime Minister, Coordinating Minister for National Security and Minister for Home Affairs

In his opening address, Deputy Prime Minister Teo Chee Hean noted that globalisation and technological advances had changed the dimensions of time, distance and complexity and, accordingly, altered the concept of national security. He urged stakeholders in security to build up anticipatory capabilities, adopt a whole-of-government response as well as work on international cooperation in order to cope with the evolving nature of national security. He noted that forums such as APPSNO could help security practitioners gain a better appreciation of the academic discourse underlying contemporary national security issues.

SESSION I: SINGAPORE'S STRATEGIC FRAMEWORK FOR NATIONAL SECURITY

Singapore's Strategic Framework for National Security

Kok Ping Soon, Senior Director, National Security Coordination Centre (NSCC), Prime Minister's Office, Singapore

Kok Ping Soon outlined Singapore's approach to strengthening national security, tracing the evolution of the country's national security framework and structures in response to changes in the operating environment. With increased complexity in the risk landscape, Singapore had to build up its repertoire of capabilities to anticipate and deal with a broadened spectrum of threats and hazards as well as adopt a whole-of-society approach to enhance its resilience against multiple national security challenges. As any framework for national security had to be contextualised to suit the current time and space on top of an understanding of the interdependent nature of risks, it was imperative to build modular capabilities to adequately deal with unforeseen events.

SESSION II: NATIONAL RISK ASSESSMENT AND MANAGEMENT – INSIGHTS FROM THE US, UK AND SWITZERLAND

Using Risk Information and Analysis to Inform Homeland Security Policy and Strategy

Alan Cohn, Assistant Secretary for Strategy, Planning, Analysis and Risks, DHS Office of Policy, USA

Alan Cohn spoke about the creation of the Strategy, Planning, Analysis and Risks (SPAR) office within the US Department of Homeland Security (DHS). He explained how SPAR integrated the DHS's strategic planning, risk modelling and analysis functions for better national risk assessment and management, an exercise largely focused on contingencies such as terrorism, national disasters, pandemics and industrial accidents. He shared the scope and the processes of SPAR's key strategic planning and risk analysis efforts like the Strategic National Risk Assessment and the second Quadrennial Homeland Security Review documents. He also highlighted the various challenges faced in developing a sound risk assessment and management framework, but underscored the usefulness of the endeavour in mapping national contingency preparedness.

National Risk Assessment in the UK

John Tesh CBE, Visiting Senior Fellow, Department of War Studies King's College, London; Former Deputy Director, Civil Contingencies Secretariat UK Cabinet Office

John Tesh CBE, presenting on national security risk assessment and management in the UK, spoke about the country's approach to building resilience to various kinds of emergencies. The UK had more recently used its risk assessment analyses for the security and safety arrangements at the 2012 Olympic and Paralympic Games as well as for the expected enduring effects that climate change could have on British society. Tesh also outlined the country's risk profiles in the mid- and long-term periods. Noting the dynamic challenges of identifying risks arising from the increased interconnectedness of the UK society and the wider world, he stressed the necessity to involve a wide range of stakeholders in the risk management process, underscoring the importance of public partnerships with the civil and private sectors.

Looking for Extreme Events in Switzerland: What Role for Risk Analysis in Critical Infrastructure Protection?

Stefan Brem, Head, Risk Analysis and Research Coordination, Federal Office for Civil Protection, Switzerland

Stefan Brem presented on the Swiss critical infrastructure protection (CIP) strategy as well as identified what was considered critical infrastructure in Switzerland, the potential risks to them and the protection process of critical infrastructures like airports and power substations. He emphasised the importance of taking a comprehensive risk approach that was about optimising security – not absolute security – based on an informed assessment of risks. He concluded that a comprehensive, all-hazard risk assessment process could help overcome major challenges stemming from CIP.

Lunch Lecture: Emergent Issues in Asian Food Security

Paul Teng, Dean, Graduate Studies and Professional Learning, National Institute of Education; Senior Fellow (Food Security), Centre for Non-Traditional Security Studies, RSIS, NTU

Paul Teng's presentation focused on emerging issues that were likely to adversely affect food security in contemporary Asia. He argued that even if the region continued to grow economically, it was in danger of experiencing food insecurity if appropriate policies and interventions were not developed soon. He explained that a variety of factors contributed to the current state of affairs: (i) an increasingly affluent and urban population and decreasing numbers of farmers; (ii) declining performance of agriculture; (iii) climate change and natural resource degradation; (iv) price volatility; (v) diversion of food/feed to biofuel production; and (vi) the transformation of food supply chains and the emergence of supermarkets. To achieve food security, Teng suggested that governments collaborate with the private sector and civil society to address the issues of availability, physical access, economic access and utilisation.

Alumni Dinner Lecture: Leadership in National Security – Applying Operational Lessons

Bernard Miranda, Director, National Maritime Operations Group, National Maritime Security System, Singapore

Drawing on lessons learned in the Republic of Singapore Navy (RSN) over the last 32 years, and currently, as a civilian working in national security, Rear-Adm (Ret) Bernard Miranda offered eight operational lessons that could be applied to leadership in national security: (i) knowing the operating space through good sense-making and intelligence; (ii) recognising threats and communicating them well; (iii) determining the rules of engagement (ROE) and recognising that while every country ran on different ROE doctrines, it was necessary to abide by key principles of proportionality, necessity, humanity and safety; (iv) winning coalitions and partnerships through building mutual trust and respect; (v) harnessing technology as a force multiplier to boost operational effectiveness; (vi) managing information through maintaining a coherent narrative; (vii) operational learning through ROE as well as training, gaming and standardising procedures; and (viii) adopting a persuasive approach towards whole-of-government collaboration.

SESSION III: STRATEGIC AND CRISIS COMMUNICATIONS

Digitally Dissuading Tomorrow's Terrorists

Richard LeBaron, Visiting Senior Fellow, The Rafik Hariri Centre for the Middle East, Atlantic Council, USA

Richard LeBaron presented on a digital communications project undertaken in the US by an interagency team from the Center for Strategic Counterterrorism Communications that had the specific goal of dissuading people from becoming terrorists. The project harnessed the expertise of intelligence, language and cultural experts who would go online to expose the weaknesses of the al Qaeda narrative and the ineffectiveness of the organisation through the use of short videos and other media forms. LeBaron explained that team members would draw from open source and intelligence materials to focus its communications efforts on those vulnerable to terrorist recruitment to create doubts in their minds. He argued that negative reactions from the terrorist propagandists indicated that such an approach had actual impact on decisions to take up violence.

Strategic Communications through Military Diplomacy: China's Approach
Xu Hui, Professor and Deputy Commandant for Academics, College of Defense Studies, National Defense University, People's Liberation Army, China

Xu Hui presented an overview of China's military diplomacy efforts, which he defined as the peaceful use of military force, as well as outlined the current challenges the country faced, noting that there were distinct communication mechanisms in place to promote mutual understanding, clear up misperceptions, build confidence and avoid conflicts during crisis situations. Xu argued that China's military joint exercises and participation in humanitarian assistance and disaster relief, among its other peaceful military endeavours, had served as a strategic approach to develop stable working relationships with major powers, forge good relations with neighbouring countries and strengthen institutionalised relationships with various multilateral defence platforms. Such efforts were however challenged by low levels of strategic trust, particularly over certain perceptions of China's rise as a major power. Territorial and maritime disputes also presented challenges to China's military diplomacy.

Strategic Communications in Crises and Emergencies: The Singapore Approach
Philip Sim, Deputy Director, Emergency Preparedness Office, Public Communications Division, Ministry of Communications and Information, Singapore

Philip Sim presented an overview of Singapore's strategic communications efforts during crisis situations with the objective of maintaining public confidence in the government, protecting the country's international image and preventing social instability. He cautioned that a bad communications strategy would result in a loss of trust in the government and could escalate into cynicism and suspicions over government actions, even panic. Using the Fukushima power plant crisis in Japan as a case study, Sim outlined the steps taken in Singapore to counter rumours that were spreading over fears of radiation particles. He noted that good interagency cooperation as well as coordination was needed to present a united front and not contribute to more confusion.

Russia and the Rise of Asia
Dmitri Trenin, Director, Carnegie Moscow Centre, Russia

Looking back on three historical case studies – the Cold War, the Russia-Georgian conflict and the Chechen insurgency – Dmitri Trenin provided a perspective into the strategic communication challenges faced by the respective governments of those times. He noted that clear channels of communication were vital for all although the channels need not necessarily be official government ones. Miscommunications could occur when conflicting sides lacked trust and in situations when governments engaged in brinkmanship. In conclusion, he said important parallels could be drawn between the cases he brought up and the current tension between North and South Korea.

SESSION IV: CYBERSECURITY

India's Cybersecurity Policy and Strategy
Nehchal Sandhu, Deputy National Security Advisor, National Security Council Secretariat, India

Nehchal Sandhu presented on India's cybersecurity strategy and underlined the growing significance of the cyber realm to India; he however also pointed out the parallel increase in cybersecurity violations. He provided insights into new initiatives the country had adopted and shared the country's National Cyber Security Architecture which rested on foundations such as simultaneous monitoring of possible threats, assurance and certification procedures, formulation of appropriate policies, and engagement with private sector and academia. He also noted the importance of international partnerships in the cyber arena.

Cybersecurity in Singapore
John Yong, Director, Infocomm Security and Assurance, Infocomm Development Authority of Singapore

John Yong discussed the growing complexity of the cyber threat landscape and Singapore's strategies to strengthen cybersecurity. He spoke of new and evolving cyber threats and the growing sophistication of denial-of-service attacks and malware technologies. He argued it was thus important to have a comprehensive national-level programme as well as robust international and public-private partnerships. Yong also highlighted Singapore's 'Masterplan 2' (MP2), a five-year information communications security plan that spanned from 2008 to 2012 that had the objective of maintaining Singapore as a secure and trusted hub. As no organisation was a "lone island", Yong underscored the importance of the ability to identify and prioritise security threats through sound risk assessment and the capacity to recognise the potential cascading impact of cybersecurity policies.

Legal Framework for Cyber Operations

Paul Ducheine, Associate Professor of Cyber Operations and Cyber Security, Netherlands Defence Academy, University of Amsterdam, the Netherlands

Paul Ducheine talked about the legal, strategic and operational framework for military cyber operations with a particular focus on the Dutch context. He discussed the roles of the government and of the armed forces in cybersecurity; the issue of legitimacy with regard to cybersecurity as a principle of the rule of law; the legal bases for governmental and military operations; and the legal regimes constraining such operations. He also highlighted the five roles the Dutch armed forces played in cybersecurity, which included protection, law enforcement, intelligence, and disruptive and constructive cyber operations. He argued that there was a need for greater training and education in order to truly understand a nation's vital interests as well as to improve understanding of various sources of cyber threats.

NATO's Cyber Defence Policy

Christian-Marc Liflander, Policy Advisor, Cyber Defense Section, Emerging Security Challenges Division, NATO HQ

Christian-Marc Liflander focused his presentation on NATO's Cyber Defence Policy against the backdrop of NATO's Strategic Concept as well as the essential role the private sector could play in ensuring effective cybersecurity. The Strategic Concept recognised that cyber attacks posed a real threat to NATO and it required a coordinated approach to cyber defence that focused on prevention, resilience and non-duplication efforts across the Alliance. The NATO Cyber Defence Policy clarified the political and operational mechanisms of NATO's response to cyber attacks and set out a framework for how NATO could assist Allies in their respective cyber defence efforts.

Distinguished Lunch Lecture: Addressing Complex National Security Challenges – Reflections of a Senior Policymaker

Peter Ho, Chairman, Urban Redevelopment Authority Board; Senior Advisor, Centre for Strategic Futures; Senior Fellow, Civil Service College; Adjunct Professor, RSIS, NTU

Basing his lecture on the post-9/11 setting, Peter Ho said that the world was only going to get more complex with unpredictable 'black swans' and highly convoluted 'wicked problems'. Ho argued that all human beings were prone to cognitive limitations such as willful blindness, hyperbolic discounting, attention bias and bounded rationality that constrained their ability to adequately deal with black swans and wicked problems. He then suggested how policymakers might learn to operate in a complex world through, among other things, war- or policy-gaming that would see the discussions of complex issues take place within a safe environment; the fostering of a coordinated whole-of-government approach to address wicked problems; the engaging of multiple stakeholders to deal with any one issue; the breaking down of vertical silos of information compartmentalisation; the establishment of structures to avoid group-think; and the creation of lean, efficient and resilient organisations that could cope with strategic shocks.

Distinguished Dinner Lecture: Addressing the National Security Challenges of the 21st Century – The Need for Better Academic-Practitioner Collaboration

Robert Hutchings, Dean, Lyndon B. Johnson School of Public Affairs, University of Texas, USA

Robert Hutchings observed that there had been a widening gap between the worlds of policy and of learning in the US and in many other countries. He believed that it was crucial to find ways to close this gap; academic disciplines needed to be made more relevant to policy making and policy makers needed to become more accessible. He also noted the importance of developing global partnerships for the study and practice of diplomacy. In a world that was in the midst of profound power shifts, Hutchings said that it was not enough to be able to identify broad emerging trends, but it was important to understand how those trends would interact with one another as well.

SESSION V: COUNTERING VIOLENT EXTREMISM AND RADICALISATION

Manichean Mindsets: What does Psychology tell us about Violent Extremists

Kumar Ramakrishna, Head, CENS, RSIS, NTU

Kumar Ramakrishna developed a concept of the "Manichean Mindset" from theories in psychology to examine how individuals could be radicalised into violent extremism. He posited that the Manichean Mindset was a default human instinctual setting derived from the unconscious tribal impulse to defend one's in-group identity or "Group Tent". Its four elements were the tendency to see the world in binary terms, the perception of the in-group as the centre of one's social universe, a distrust of out-groups, and the desire for one's Group Tent to be higher in the social pecking order than the out-groups'. He argued that extremists who positively accepted violence in politics possessed an amplified Manichean Mindset. Such individuals were often fanatically closed-minded, accepted democratic processes only as a stairway to power, were supremacist, authoritarian, intolerant and dogmatic in outlook, rejected equality, diversity and human rights, and embraced the use of political violence. Ramakrishna concluded that effective measures to counter violent extremism should not only focus on counter-ideological programs and law enforcement but also on preventing the innate Manichean Mindsets from radicalising into cognitive extremism through a deliberate process of personalising, de-categorising and humanising out-groups.

Academic Input and the RRG's Counter Radicalisation Programme

Mohamed Feisal bin Mohamed Hassan, Associate Research Fellow, ICPVTR, RSIS, NTU

Mohamed Feisal Bin Mohamed Hassan shared the experience of Singapore's Religious Rehabilitation Group (RRG) in winning the hearts and minds of radicals and extremists and inoculating the community from radicalisation. A key pillar of the work of the RRG was religious counselling for extremist detainees, an endeavour that involved extricating negatively imbibed ideology, replacing negative ideology with positive ones, imbuing a rightful understanding of Islamic knowledge and exemplifying fulfilling ways of living in a multi-racial, multi-religious society. Beyond the focus on detainees, the RRG would also offer community support to detainees' families and conduct public outreach programmes that drew on academic insights through the RRG's partnership with various academic institutes. Mohamed then highlighted five challenges facing the RRG: the phenomenon of self-radicalised individuals, the harnessing of social networks by radical groups, the proliferation of radical internet ideologues, and the broadening of radical propaganda to reach out to English-speaking audiences.

Utilising Academic Approaches in Counterterrorism: The Detachment 88 Experience

Muhammad Tito Karnavian, Chief of Police, Papua Province, Indonesia

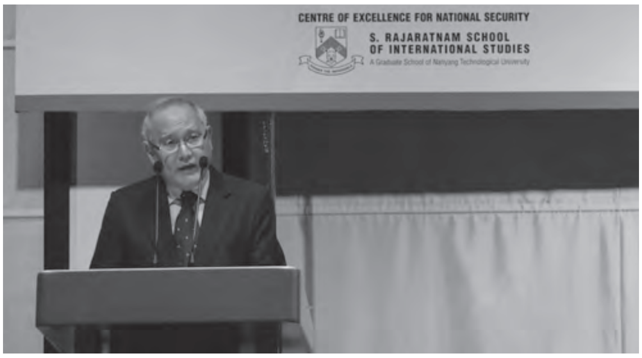
Muhammad Tito Karnavian assessed the successes and challenges faced by Indonesia's Detachment 88 when employing academic approaches to counterterrorism. Recognising that tactical law enforcement operations alone were insufficient to contain the terrorist threat, the unit developed a broader understanding of terrorism to neutralise the complex threat more effectively. Academic lenses and methods were employed to assess terrorist groups, new trends in terrorism and best practices in counterterrorism strategies in Indonesia and beyond, leading to the development of a strategic and operations framework grounded in a law-enforcement approach. Other measures informed by academia included the adoption of soft measures in engaging radical individuals and the wider community, and systematic approaches to neutralising recruiters, radical ideology and underlying causes of terrorism. Some challenges were also identified, namely determining relevant/appropriate methodologies and best practices to adopt and the imperative for better collaboration between academics and practitioners.

Saudi Efforts in Counter-Radicalisation

Abdulrahman AlHadlaq, Director General, Ideological Security Directorate, Ministry of Interior, Kingdom of Saudi Arabia

Abdulrahman AlHadlaq presented on the Saudi strategy of Prevention, Rehabilitation and After-Care (PRAC) to counter radicalisation and extremism. The strategy comprised three interconnected programmes: the first focused on preventing the spread of violent radical ideology by rectifying misunderstandings about Islam alongside the propagation of moderate Islam through various media outlets and engagement with religious institutions, educational institutes and civil society. The second programme provided rehabilitative counseling and care to extremist detainees with the goal of replacing their extremist ideology with a moderate one and to prepare them for reintegration into Saudi society after their release. The third programme was the after-release care programme to facilitate the reintegration of released detainees into society. Drawing lessons from the Saudi experience, AlHadlaq concluded that comprehensive strategies, adequate resources, sound programmes and evaluation processes, and international cooperation were crucial.

OPENING REMARKS


CENTRE OF EXCELLENCE FOR NATIONAL SECURITY
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
A Graduate School of Nanyang Technological University

Ambassador Barry Desker

In his opening remarks, Ambassador **Barry Desker** welcomed all participants to the 7th Asia-Pacific Programme for Senior National Security Officers (APPSNO). Initiated in 2007 as a forum to bridge the gap between the theory and practice of national security, the current APPSNO was dedicated to the theme of "Narrowing the Theory-Practice Gap". Participants could look forward to discussing practical ways in which policy practitioners could deal with evolving national security challenges through effective partnership with the academic community. With national security matters becoming ever more complex, the best solutions needed to come from a synthesised academic and policy world.

Ambassador Desker further showcased how RSIS had long attempted to amalgamate the worlds of academia and policymaking. He noted that different research constituents of the School had developed good working relationships with several state agencies in Singapore. CENS' role as the academic partner of the National Security Coordination Secretariat in the Prime Minister's Office was highlighted as one example of this kind of mutually – beneficial partnership. With APPSNO 2013 featuring discussions on national risk assessment and management, strategic and crisis communication, cybersecurity, and approaches to counter violent extremism and radicalism, Ambassador Desker believed that APPSNO was well-placed to be the forum in the Asia-Pacific region where national security practitioners could learn and relearn their skills through networking and active engagement. He hoped that all the participants would gain important lessons from the week to come that they could later put into practical use.

OPENING ADDRESS

Deputy Prime Minister Teo Chee Hean

In his opening address, Deputy Prime Minister **Teo Chee Hean** said globalisation and technological advances had changed the dimensions of time, distance and complexity, and accordingly, revolutionised the concept of national security. The focus of national security had expanded beyond building military capabilities to safeguard territorial integrity; there were also need for social, economic, energy and food security.

DPM Teo noted that threats to national security could come from many places. Transnational crime syndicates, terrorist groups and online hackers were highlighted as several contemporary examples of security threats stemming from non-state actors. He further cautioned that some threats could develop within a short period of time and their fallouts might be omnidirectional, causing interconnected failures instead of the disruption of singular, predictable targets. Three varied examples were drawn upon to buttress his point: (i) the rapid spread of the Severe Acute Respiratory Syndrome (SARS) virus in 2003 infected over 8,200 individuals in nearly 30 countries and killed over 770; (ii) the eruption of the Icelandic volcano in 2010 disrupted over 95,000 flights in Europe, and by day six, the loss in revenue amounted to more than $1.7 billion; and (iii) the denial-of-service attacks on Spamhaus spam blocker slowed down Internet access worldwide for more than a week, underscoring how the networked and complex nature of cyberspace could allow cyber attacks to be conducted anonymously from abroad, affecting everyday activities.

In light of the complex challenges to contemporary national security, DPM Teo pointed to the importance of new theoretical approaches to thinking about such issues and fresh strategies to put into practice. First of all, he underscored the necessity of building up anticipatory capabilities through environment scanning and the exchange of information and intelligence. This, he argued, would allow practitioners to anticipate possible threats and formulate actions to respond to them. The Safe City Testbed initiative was mentioned as an example of how Singapore sought to boost its anticipatory capabilities; by setting up testbeds that integrated advanced analytics into existing sensors and systems of government agencies, information from various sources could be correlated, thus aiding the tracking and deployment of resources on the ground.

Secondly, DPM Teo called for the adoption of a whole-of-government, even a whole-of-society response to tackle omnidirectional and interconnected contemporary threats. Singapore's response to the SARS epidemic was highlighted as a good example of a multi-pronged management of a threat that involved numerous agencies from the public, private and civil sectors.

Finally, DPM Teo noted the importance of international cooperation to cope with the evolving nature of national security. International collaboration on cybersecurity, for instance, would ensure the development of effective responses to security challenges in the cyber arena. To this end, the new INTERPOL Global Complex for Innovation which would open in Singapore in 2014, would help facilitate cyber research and innovation as well as provide cyber training and operational support for law enforcement agencies. DPM Teo concluded that forums such as APPSNO would help security practitioners gain better insights into the academic discourse underlying contemporary national security issues.

SESSION I:
SINGAPORE'S STRATEGIC FRAMEWORK FOR NATIONAL SECURITY

Kok Ping Soon

Kok Ping Soon presented on Singapore's national security framework and traced its evolution in response to changes in the operating environment. With increased complexity in the risk landscape, he said Singapore had to build up its capabilities to anticipate and deal with a broadened spectrum of threats and hazards, as well as adopt a whole-of-society approach to enhance its resilience against multiple national security challenges.

Kok pointed out that the national security framework had been contextualised to Singapore's unique geographical and historical conditions. The island state's small size, for instance, proved a double-edged sword. On one hand, it meant that Singapore was able to react quickly to changing situations, but on the other hand, the corresponding small size of its military force meant defense could be challenging. However, making up for the size deficit was the constant improvement of military technology capabilities. Singapore furthermore saw diplomacy and security in a complementary relationship and thus placed strong emphasis on the former in its conduct of foreign affairs, cognisant that that might lead to the reduction of threats to security. Moreover, as Singapore generally understood the interconnectedness between security and internal stability, social development was also a priority.

Kok proceeded to highlight three shifts in Singapore's evolving security landscape. The first was with regard to a shift in the source of national security threats from one to many. That meant there could be problems recognising what kinds of threats would materialise and which ones to pay attention to. To this end, national security officers from nine different agencies in Singapore came together for an exercise in 2012 to identify multiple issues threatening national security and establish their risk statuses; the plotting of this segmented risk map was meant to inform capability development and contingency planning.

Secondly, Kok observed that the nature of risk had evolved from distinct to interdependent. For instance, the 2011 floods in Bangkok not only affected the daily lives of the Thais, but also affected the global automobile industry. In light of the interdependent nature of risks, Singapore set up the Risk Assessment and Horizon Scanning (RAHS) programme in 2004 to explore tools and methods that could complement scenario planning to anticipate issues that impacted national security.

Finally, for security to be comprehensive, a whole-of-society approach was necessary. Advancement in information communications technology had provided citizens more ways and avenues to become more vocal in articulating their views, and turning such into a force for good was a concern of policy practitioners. Continuing to commemorate events such as Total Defence Day would continue to instill a sense of shared nationhood among Singaporeans. In addition, the promotion of community engagement through outreach efforts to religious groups, schools and the media would lead to racial and religious harmony and social resilience.

In conclusion, Kok noted the importance of building up modular capabilities as unforeseen events and issues would persist in surprising policy practitioners. There was also a need to integrate and coordinate across operatives and technological platforms. Additionally, anticipatory capabilities should be developed and a whole-of-society approach should be adopted when dealing with national security.

Discussion

A participant asked if the Singapore government had a list of possible threats to national security that it could share. The speaker said there were plans to release the full list of national security risks, but the date to do so had not been agreed upon. That said, concerns over border security, homegrown terrorism and the problem of self-radicalisation currently ranked as high priority issues. He added that the National Security Coordination Secretariat was doing its part to look for possible gaps between incidents and what they could do about it; the agency was committed to finding common areas for cooperation and solutions. As national security threats constantly evolved, national security officers would always find their work to be perennially "in-progress".

Another participant asked what constituted the greatest challenge to resilience and what could be the kinds of measures that were needed to achieve it. The speaker responded that the notion of resilience could fall into two broad categories: hard and soft. Social resilience – falling under the latter category – was considered the most difficult to build. A society would be more united if there was a network of trust, but that was something that had to be cultivated during times of peace. Yet, what specific elements constituted social resilience would continue to be debated as they were highly dependent on context.

SESSION II

NATIONAL RISK ASSESSMENT AND MANAGEMENT – INSIGHTS FROM THE US, UK AND SWITZERLAND

7TH ASIA-PACIFIC PROGRAMME FOR SENIOR NATIONAL SECURITY OFFICERS
8TH - 12TH APRIL 2013
Opening Address by Mr Teo Chee Hean
Deputy Prime Minister, Coordinating Minister for National Security and Minister for Home Affairs
NSCS

(from left) Alan Cohn, John Tesh CBE, Stefan Brem and Kok Ping Soon

Alan Cohn, presenting on national risk assessment and management from the US perspective, started with a brief introduction to the Department of Homeland Security (DHS) and the DHS Office of Strategy, Planning, Analysis and Risk (SPAR). He explained that the DHS was established in the wake of the 9/11 attacks, and in 2012, the Department merged its strategic planning and risk analysis offices to form the SPAR office. The office was designed to elevate the importance of a strong risk modelling, analysis and strategic planning function within the DHS.

Cohn then provided an overview of two exercises conducted by the SPAR office: (i) the Strategic National Risk Assessment (SNRA), and (ii) the Homeland Security National Risk Characterisation (HSNRC). The SNRA looked at contingencies such as natural disasters, acts of terrorism, pandemics and industrial accidents. Cohn pointed out that the main lesson learnt from the exercise was the essentiality of having an executive mandate. Having the US president sign a presidential policy directive on national preparedness that included a mandate to conduct strategic national-level risk assessment to inform national preparedness capabilities targets was paramount for the endeavour.

In relation to the methodology of risk assessment, Cohn explained that likelihoods and consequences were considered. Likelihood, which included the level of threat and vulnerability, was typically measured in terms of frequency or probability. Consequence featured six categories of impact: fatalities, injuries and/or illnesses, and economic, social, psychological and environmental impact. Cohn emphasised that not all assessments of risks looked at the consequences the same way so it was therefore important to fully understand the different terms and what they meant. Further, although it was desirable to have an order of the magnitude of all risks, such precision was simply not possible; rather, identifying the few risks that stood out was more optimal.

The HSNRC exercise comprised of placing contingency risks on a similar continuum with persistent risks like transnational border crime, human and narcotic trafficking, and mass migration to see if comparisons could be made with regard to the relative level of risk caused by these essentially dissimilar risks. Cohn said such an exercise drove home the point regarding the criticality of definitions; it was necessary to ensure clear distinctions were made between what would be considered catastrophic events and what were risks faced on a day-to-day basis. He also emphasised that there was really no breakpoint between persistent and contingency risks; instead, there was a continuum of frequencies.

Cohn stressed that the results from such analyses had to be directly applicable to the decision-making process. He said that it was fairly easy to fall into the assumption that assessment exercises were purely for technical or analytical reasons that had no regard for operational or political concerns. When conducting such exercises, it was thus essential to look at a wide range of risks, find thresholds, identify uncertainties, build risk profiles and look at those that stood out; the conclusions derived based on risk calculations could then be communicated to a wider audience. Cohn concluded that risk assessments could be a snapshot in time, but they were nevertheless useful to examine current trends, future uncertainties and causal relations.

John Tesh, having been involved in risk assessments at the national level as well as on climate change and the 2012 Olympic Games in London, presented on national risk assessment from the UK perspective. At the outset, he underscored the importance of clarity in knowing the exact purpose behind such assessments, and for the UK, the goal of such endeavours was to enable the government to control risks and manage emergencies in the country. Emergencies were defined as events that could cause or threaten to cause significant harm to human welfare or the environment. He added that the national risk assessment was focused on domestic concerns and examined a limited horizon of up to 5 years.

The national risk assessment incorporated hazards such as terrorism and man-made accidents, but not day-to-day incidents such as crime or traffic accidents as they did not meet the definition of contingency. Tesh shared that the national risk assessment from 2012 saw pandemic influenza, coastal flooding and effusive volcanic eruption as the main identifiable natural hazards in the UK. The only threat identified as catastrophic was terrorism, whereas cyber attacks and attacks on infrastructure, in crowded places or on the transport system, were identified as high-range threats.

Tesh said that while it was useful to catalogue current risks for the UK, assessments would be of better utility if they could give a sense of where such risks were going in the longer term. This subsequently led to a longer term horizon scanning in order to see how short term domestic risks could likely develop in the long run. There was cognition that the UK risk profile could be expected to be affected by things like climate change and global instability as much as domestic elements such as the networked and interdependent nature of the British society. Such dynamics could increase the risks of cascade failures.

Accordingly, on request of the UK government, a 20-year strategic risk assessment which incorporated a global perspective was undertaken. The objective of the exercise was for the government to receive strategic notice of future risks. The national risk assessment looked at four main areas that were classified as tier-one risks: (i) international terrorism; (ii) natural hazards, particularly in those areas affected by climate change; (iii) hostile attacks on the UK cyberspace by other states and large-scale cybercrime; and (iv) international military crisis drawing in the UK, its allies as well as other states and non-state actors.

In relation to the climate change risk assessment, Tesh spoke about the opportunities and threats stemming from climate change. He explained that although the assessment looked into opportunities resulting from warming weather conditions, the threats yet remained far more serious. Specifically for the UK, he said the threats stemmed from droughts, coastal flooding as well as the lack of water supply.

Stefan Brem provided an overview of the Swiss risk analysis in critical infrastructure protection (CIP) and pointed out three core elements to the CIP. Firstly, there was a clear definition of what was considered critical; there were ten different categories of critical sectors, with some being further subdivided into subsectors. Secondly, a hazards approach that looked at varied relevance of different hazards to different sectors and subsectors was utilised. Thirdly, there were comprehensive sets of measures that could address specific threats. The central aim of the CIP exercise was to prevent breakdowns, and if something were to happen, to reduce possible damage.

Brem pointed out that the mandate for the implementation of the 2012 CIP Strategy was provided by the Federal Council. The overarching goal of the programme was to improve the resilience of critical infrastructure in Switzerland through coordinated and unified approach of all stakeholders. The basic principles of the programme included a comprehensive risk-based approach; proportionality, in reflecting the understanding that not everything could be protected at all times but that prioritisation was needed; responsibility of the actors involved; and public-private partnerships as essential components, particularly when it came to burden and information sharing.

As a way to formulate the CIP strategy, the inventory of the Swiss critical infrastructure objects was mapped. It was to form the basis for planning and prioritisation of risk and disaster management in the confederation and the various cantons. Throughout the mapping process, what was also taken into account was the question of whether the failure of such infrastructure would have impact on the regional or national level.

With regard to the prioritisation process, Brem explained the five steps involved: (i) the creation of functional structures within each sector wherein the main production and distribution lines were examined together with the how the processes were handled; (ii) determine the relevant object groups, i.e., power plants, important routes, etc.; (iii) identify the threshold levels for all subsectors; (iv) evaluation of critical infrastructure objects that focused on the output potential of different objects, i.e., how many goods could be produced, distributed or consumed, as well as the hazard potential of certain plants and infrastructure; and (v) after completion of the national inventory, the same inventory mapping would be done at the cantonal level. Brem pointed out that the Swiss approach was similar to the EU's; the only difference was in terms of priority regarding levels of assessment being on the national level instead of a regional one.

Based on the final hazard catalogue, risk diagrams were drawn along with a list of different categories of hazards. Natural hazards referred to occurences like earthquakes, inland flooding or windstorms; technical hazards included electricity outages, road accidents with dangerous goods; and societal hazards meant man-made attacks using dirty bombs or chemicals like sarin, cyber attacks, pandemic animal diseases or mass migration. To conclude, Brem listed the twelve indicators that had been developed based on the federal constitution to assess damages in the hazard aftermath.

Discussion

A participant noted that since risks could come from anywhere, a more integrated and participatory approach to risk assessment and management was needed, particularly in relation to data collection and risk communication; he asked if the speakers could further explain how a more coordinated approach involving inter-sector cooperation as well as inter-governmental cooperation could be achieved. The speakers responded that while data collection and information sharing regarding potential threats between and among governments were great areas for opportunities to cooperate, it remained that different governments had different views and gave different weight to different kinds of threats.

Regarding risk communication, one of the speakers explained that some community resilience programmes included exercises that involved inviting volunteer groups to help in a hazard aftermath. These volunteers would come away from the experience understanding the actual impact that certain hazards could have at the local level. Such an endeavour helped increase awareness among the local population as well as encourage more active involvement in threat reduction and management.

LUNCH LECTURE

EMERGENT ISSUES IN ASIAN FOOD SECURITY

Paul Teng

Paul Teng began his presentation by defining food security as a situation where "all people at all times have physical, social and economic access to sufficient, safe and nutritious food that meets their dietary needs and food preferences for an active and healthy life". He maintained that food security was highly dependent upon four main criteria: (i) food supply – in terms of availability; (ii) access to food – in terms of the market supply chain; (iii) economic access to food – in terms of income to purchase food; and (iv) food utilisation – in terms of the safety, quality and nutritive value of existing food supplies.

Teng went on to list a number of factors that had negative impact on global food security. Among them were: demographic changes; poverty; underinvestment in infrastructure and technology; climate change; degraded natural resources base; unfriendly policies towards farmers; declining number of farmers; globalisation; severe weather disruptions; natural calamities; pest and disease outbreaks; rising energy prices; competition from the energy sector; sudden policy changes; diversion from staple to cash crops; conflict/terrorist activities; economic factors; price hikes; food safety/contamination; alternative uses of biomass; and human health crises (e.g. SARS).

Several trends further suggested that food insecurity could soon become a reality in Asia. Demographic shifts saw to high population growths, and that combined with urbanisation and an overall increase in GDP per capita, had led to significant changes to existing diets. This, in turn, had led to an increase in demand for greater food variety. The declining performance of agriculture, too, increased pressure on the natural resources base thereby creating a demand for new paradigms and technologies. In addition, environmental degradation and climate change had not only reduced food production but also destabilised it. Furthermore, increases in oil prices and biofuel expansion had reduced crop productivity and land use substitution. The rapid transformation of supply chains was also a cause of concern.

Teng made several suggestions to address these challenges. With regard to availability, it was imperative to increase agricultural productivity, reduce waste, encourage sustainable international trade, and review agricultural/biofuel policies. In relation to physical access, a reduction in waste was needed as well as improvements to transport and infrastructure. Also, the linkages between farmers and markets needed enhancement. With regard to economic access, new social programs and safety nets had to be developed in addition to increasing the entrepreneurial skills of farmers. Furthermore, creating non-farm employment was important as well. In terms of utilisation, bio-fortification, the introduction of dietary supplements, monitoring of nutritional security progress and overall improvements made to education, healthcare, infrastructure, hygiene and food safety were paramount.

Discussion

A participant enquired about the prospects of biofuel becoming an alternative energy source. In response, Teng said that while many countries were seriously considering its use, it was less deliberated in Asia. He believed that Asian countries should consider using biofuel and suggested that interested countries grow crops that could support the industry. However, he cautioned that such crops should not compete with crops grown for food.

3rd APPSNO ALUMNI DINNER LECTURE

LEADERSHIP IN NATIONAL SECURITY: APPLYING OPERATIONAL LESSONS

Bernard Miranda

Drawing on lessons learned in the Republic of Singapore Navy (RSN) over the last 32 years, and currently as a civilian working in national security, **Rear-Admiral (Ret) Bernard Miranda** began by outlining the national security challenges in the Asia-Pacific. The regional security architecture that was taking shape was being defined by new emerging powers, demographic and social changes, increasing demand for energy and resources, territorial disputes, rapid growth rates and transitions in leadership.

To navigate these complex challenges with a sense of reality, Miranda offered four suggestions drawn from his operational experience in the Gulf of Aden, summarised in the acronym BEER: Building awareness, Engaging partners, Enhancing relationships, and Responding promptly and appropriately. Elaborating on BEER, Miranda explained that leadership in national security involved providing a strategic operational context, enhancing relationships, setting clear and achievable goals and directions, having command and control over operations, and optimising scarce resources.

Miranda then outlined eight applicable lessons for national security operations:

(i) Know the operating space. That meant operations, intelligence and administration staff should have a collective appreciation of the geography, history and culture as well as the security challenges of the locality they were operating in whilst also understanding how global influences could have impact on the local space. In that respect, sense-making and intelligence were important;

(ii) Recognise threats. To do so, good sensors, information sharing, timely intelligence and sense-making of suspicious activity were required, and friendly help and effective communication were essential;

(iii) Determine rules of engagement (ROE). Every country had different ROE principles, accordingly making it important to distinguish between civilian and military objectives and keeping to a graduated but timely approach in engaging the enemy by applying the principles of proportionality, necessity, humanity and safety;

(iv) Win coalitions and partnerships. Building diverse multinational and interagency relations meant being able to take advantage of diversity, and forging mutual trust and respect needed energy, patience and persistence;

(v) Harness technology. It was crucial to innovate and exploit technological advances such as the unmanned surface surveillance and tracking devices to improve operational effectiveness because technology was a force multiplier;

(vi) Manage information well. Keeping a tight media cycle, maintaining a coherent narrative and utilising social media were necessary to shape perception;

(vii) Operational learning, i.e., tactical guides, doctrines, gaming, training, standard operating procedures and planning processes were important although establishing the ROE was priority;

(viii) A persuasive approach towards whole-of-government collaboration, building credibility, establishing common goals and capturing mindshare was essential for leadership in national security.

Discussion

Of interest during the discussion session was the concept of graduated process of engagement. The speaker was asked why a graduated process of engagement against pirates spotted at sea would be favoured over taking immediate actions against them as well as how battle lines could be communicated to the pirates using such an engagement process. In response to the first question, the speaker explained that while the Navy could identify and pinpoint pirate activities, most of the illicit organisation and operation, however, took place on land where the Navy had no authority to operate. Even at sea, there would be a lot of capture and release because those suspected to be pirates might not have been intercepted in any act of piracy. The Navy would nevertheless still have the authority to mark suspected pirate vessels so they could be tracked and spotted from air by helicopter. Added measures like discarding weapons discovered on suspected pirate vessels overboard, installing trackers on their boats and confiscating their mobile phones and GPS units for further forensic investigations had helped stem potential pirate attacks in the absence of actual piracy. Regarding the drawing of battle lines, the speaker explained that such lines would be made clear. A line of smoke floats would be dropped by helicopter to deter the pirates, failing which, warning shots by machine gun would be fired; a final stage included having a sniper shoot at the engine of the pirate vessel from a helicopter.

On the relationship between piracy and international organised crime syndicates, the speaker alluded to the links between the two considering that the piracy ecosystem was made up of so many different players, from those who would play the role of watchdogs on the ground to the pilots who would help deliver the ransom notes. In the Somalia context, for instance, there might be ringleaders with operations in the country, but at times the actual ransom negotiators might be operating from another.

SESSION III
STRATEGIC AND CRISIS COMMUNICATIONS

(from left) Richard LeBaron, Xu Hui, Philip Sim, Dmitri Trenin and Yolanda Chin

Richard LeBaron presented a case study of a digital communications project in the US that had the objective of discouraging young people from being influenced by the al Qaeda narrative and pursuing a path of violence and terrorism. He explained that the initiative, conceived in September 2010, came about as a result of a realisation that strategic communication efforts to undermine violent extremist sentiments had thus far been sidelined and regarded a "sideshow" in anti-terrorism strategies. Contributing to that, he believed, was also the shift in perception that the so-called global war on terrorism was less about an ideological conflict than it was about regional conflicts involving small groups of people.

A central thrust of the project was about rectifying misperceptions about the US as a superpower that did whatever it pleased, a message particularly communicated to a specifically targeted online audience made up of supporters and potential supporters of terrorists. The project tapped into the expertise of retired intelligence agents, linguistic experts and academics who were familiar with evolving al Qaeda narratives and had contextual understanding of their targeted audience. Operating in digital spaces frequented by supporters and potential supporters of terrorists, the teams of experts worked to: (i) contest violent extremist sentiments online; (ii) redirect or "nudge" the online conversations towards a more desired direction; and (iii) unsettle terrorist organisations and their supporters. That said, the aim of the project was ultimately about dissuading individuals from going down the path of violence and not about convincing them of the merits of US policies.

LeBaron admitted, however, that measuring the success of the initiative was difficult, its impact apparent only to have a correlative effect rather than a causative one. On top of that, he noted two important exogenous factors that had tremendous bearing on dynamics on the ground: the Arab Spring and the death of Osama bin Laden. With the Arab Spring, people became less interested in what al Qaeda had to say, and the death of bin Laden and other key al Qaeda figures further weakened the group's sway.

Outlining lessons learnt, LeBaron said that, firstly, undermining the legitimacy of al Qaeda was critical as it would create doubts in the minds of those who were contemplating going down the path of terrorism. Secondly, selecting the right people for the expert team was also important because they needed to possess great language skills to effectively communicate with and engage their targeted audience; they needed good analytical skills, too, that reflected sound understanding of the different contextual realities of the individuals they were in contact with. Thirdly, strong interagency cooperation as well as a supportive leadership was required for the maintenance of such a project. LeBaron concluded that as terrorism would continue to persist, the further development and undertaking of such communication initiatives remained a necessity.

In his presentation, **Xu Hui** explained the concept of military diplomacy and outlined China's efforts at building confidence, establishing common security and achieving cooperative security through the peaceful use of its military force. He reiterated that the military would use force as a last resort should diplomacy ever fail, but China's military diplomacy efforts had thus far strategically communicated the country's foreign policy of peace. That the Chinese military had not been involved in war in the last three decades was evidence of its peaceful intentions.

Xu provided a historical review of China's military diplomacy efforts and highlighted three distinct phases. The first phase was between 1949 and 1970, a period for the military that was dominated by the themes of war and revolution, and its policies reflected such dynamics. At the time, it was felt that there was a need to distinguish enemies from friends, and under the circumstances the priority was to build military alliances to safeguard the national and international interests of socialist countries in order to prevent the threat of war and/or invasion. The second phase, between the 1980s and the early 2000s, marked a time of reform. The foremost themes of the time was peace and development; the period also saw to an evident refrain of the use of force in territorial disputes. Additionally, as a formal member of the United Nations, China had embraced the need to forge mutual understanding, build confidence, and promote peace and stability. Finally, in the third phase, which was from the turn of the century to the present, the approach adopted by China had been one of peaceful development. With globalisation and increasing interdependence, China's military diplomacy efforts had been vital to the country when it came to deepening international relations and maintaining regional peace and stability. Trust and confidence had also been enhanced through military endeavours such as defence consultations, professional exchanges and joint exercises, participation in humanitarian assistance and disaster relief, and peacekeeping operations.

However, while China's military diplomacy had helped promote mutual understanding, he noted that there remained gaps in knowledge and perception about China, which was why public communications to clear misunderstandings regarding its nature and intentions was important on both the strategic and the operational levels. One of the main challenges to China's military diplomacy remained mutual mistrust between China and certain countries over ideological variances and different security conceptions. China's rise was thus often of concern and perceived to be a threat. Military diplomacy efforts were also impacted by territorial and maritime disputes between China and its regional neighbours. Nevertheless, military diplomacy remained important because it had contributed to conflict avoidance when disputes escalated to a point of crisis. Xu pointed out that one of the fundamental principles in crisis management was keeping communication lines open at all times and to convey clear and coherent messages to the other side in timely manner. In conclusion, Xu noted the importance of effective strategic communications between countries in order to achieve peaceful development for all.

Philip Sim outlined the importance of effective crisis communication for governments. Firstly, effective crisis communications could help maintain public confidence in the government. Where there was public confidence, government agencies would have the luxury of additional time and space to assess and manage a crisis, which at times might necessitate the implementation of severe measures. Secondly, effective crisis communications would protect a country's international image. Speaking about the local context, Sim said a lack of confidence in Singapore in the aftermath of a crisis would dissuade companies and individuals from coming to do business and that would severely affect the country's economy. Thirdly, depending on the nature of the crisis, effective crisis communications was crucial to prevent possible social fissures from developing in the crisis aftermath. The preservation of social cohesion in a crisis situation could not be more important.

In an event of a crisis, different government agencies would expectedly provide information to the public regarding their respective areas of responsibilities, and with many involved in the process of releasing information, there was risk of sending out contradictory messages. In such a case, agencies might appear uncoordinated, or worse, unable to handle the crisis, leading to an additional crisis of waning public confidence. Sim metaphorically likened public confidence to money in the bank; such vital assets needed to be garnered and saved during times of quiet so there would be ample reserves to draw from during crisis situations.

In Singapore, Sim explained that the Ministry of Communications and Information was tasked with coordinating communications across all agencies as soon as a crisis occurred. A task force comprising key officers within the ministry would be formed. The task force would report directly to senior civil servants handling the crisis and would provide support to other agencies in terms of: (i) sense-making of pertinent issues of concern to the public; (ii) offering comprehensive assessment of actions to be taken, including elements in the planning process, what channels of communications to use, and messaging coordination; and (iii) in the execution stage. The Fukushima Daiichi nuclear power plant crisis of 2011 showcased that although Singapore saw little or no direct impact from it, rumours about radioactive particles floating in the air began circulating nevertheless. In response, having assessed that such rumours could cause unfounded fears, a crisis management group was activated to address the issue. The Ministry's task force came up with recommendations and a coordinated response to guide the various agencies involved in disseminating relevant information to the public. Of priority was coordination between the agencies to prevent incongruous messages from being released to the public. Such coherence gave clear indication that the government was on top of all possible fallouts and had in place necessary precautionary measures should they be needed.

Sim concluded with the observation that in the age of social media, social networking tools such as Twitter and Facebook were useful communication tools, and interagency coordination would become ever more crucial for effective, well-organised communication.

Looking back on three historical case studies – the Cold War, the Georgia-Russia crisis and the Chechen insurgency – **Dmitri Trenin** provided a Russian perspective of the strategic communication challenges faced by the incumbent governments of the time.

During the Cold War, the Cuban missile crisis stood out as an important case study for strategic communications. A key lesson learned from the incident was that adversaries should not be demonised. Instead, every effort should be made to understand how any particular crisis was viewed and understood by the other side. The world had almost come to the brink of a nuclear confrontation because the two superpowers of the day attempted to outmaneuver the other; the crisis began when it was discovered that the Soviet leadership had started installing secret nuclear missiles facilities in Cuba in its attempt to counter the US.

Another key lesson that could be drawn from the crisis was the necessity of having operational channels of communication between the two conflicting sides. Trenin noted that the most effective lines of communications during the crisis were not official ones, but rather, it was one that existed between a Soviet intelligence officer based in Washington and Robert Kennedy, the brother of the late US President John F. Kennedy. Such a channel allowed communications to reach both leaders across the Cold War divide, which eventually played a significant role in diffusing the 1962 crisis.

Even with today's modern, fast, clear and direct lines of communications, incidences of miscommunication could still occurr, as was evident during the Georgia-Russia crisis of 2008. Russia and the US had seemingly come close to a major crisis which was rooted in the decision taken by members of the North Atlantic Treaty Organisation (NATO) to include Georgia into their fold. Russia had understood that the US favoured the inclusion of Georgia as a NATO member, and along with the increase in the number of border incidents between the Georgian forces and the Russian-supported separatist forces in Abkhazia, miscommunications became increasingly ubiquitous. Trenin argued that the border skirmishes conveyed two messages in terms of strategic communications: on one hand, they raised questions over the suitability of Georgia's NATO membership while, on the other hand, Georgia used the threat it faced to underscore the need for the country's inclusion into NATO. Trenin noted that tensions tided over in the end, but one of the main lessons learnt from the incident was that brinkmanship could get out of hand. The incident also saw a severe lack of trusted communication sources on both sides.

In relation to the Chechen insurgency, Trenin highlighted how Russian President Vladimir Putin recognised several elements central to strategic communications. Putin communicated clearly to the Russian people about the need to confront the threat of insurgency and to stand behind the government's policies and the country's troops. He showed himself resolute, and that sent the message to both the people and the insurgents that he would take very decisive actions. As a result of his actions, there was stability in the region although insurgency continued a problem.

Trenin concluded saying that while history never repeated itself there were lessons to be drawn. The Cuban missile crisis, for instance, proffered some parallels for the current tension between North and South Korea.

Discussion

A question about the role state leaders and politicians could play in crisis communications was raised during the discussion session. One of the speakers said state leaders and politicians could prove to be highly effective spokespeople, but their participation in crisis communications must be carefully thought through prior so as not to give the unnecessarily perception that a situation was graver than it actually was. Hence, an important aspect of effective crisis communication was in deciding whom to have as a key spokesperson.

A participant also asked whether there were attempts to analyse how terrorist groups constructed their narratives and exerted influence over individuals. A speaker responded that there had been a lot of effort put into understanding narratives and how they could move. However, what was more important was in figuring out how to counter the narratives found online in much the same way any commercial company would if they were confronted by negative feedback or hit by rumours.

Another participant asked whether the messages relayed in a crisis situation for the sake of strategic communications had to always be the complete truth. One of the speakers replied that while, in principle, telling the truth should always be upheld, it remained important to bear in mind the decisions regarding which facts and information to release to the public required some judgment. The untimely release of some kinds of information, for instance, could lead to undesired reactions like unnecessary panic or anger. Nevertheless, sharing important developments during a crisis was always important because not doing so could adversely affect levels of public trust should it be later discovered that pertinent facts were not made available when it should be by the government. Another speaker added that sending a clear message was of paramount importance; it was also necessary to consider exactly who the target audience was and whether the message was meant for a domestic or international audience.

SESSION IV
CYBERSECURITY

7TH ASIA-PACIFIC PROGRAMME FOR SENIOR NATIONAL SECURITY OFFI
8TH - 12TH APRIL 2013
Opening Address by Mr Teo Hean

(from left) Nehchal Sandhu, John Yong, Paul Dechaine, Christian-Marc Liflander and Caitriona H. Heinl

Nehchal Sandhu presented on India's cybersecurity strategy. He first provided an overview of India and then elucidated the importance of cyberspace to key critical sectors in the country. Noting the growing threat of cyber attacks, he outlined a number of new initiatives the country had undertaken to counteract threat trends in the cyber arena.

Sandhu noted that an increasing number of Indians had access to the Internet every year as reflected by the growth of smartphones and the widespread use of social media sites. He further pointed out that the number would only continue to rise nationwide with the government intent on expanding Internet connectivity to more rural areas. With such technological advancements and increased access, however, vulnerabilities in cyberspace were naturally going to see a corresponding increase. In the past five years, India's Computer Emergency Response Team reportedly had to deal with a 700% increase in illegal cyber activities, with 18,000 incidents occurring in 2012 alone. Motivations behind such cyber activities varied widely, from mobilising agitators against government policies to defacing websites, online stalking, impairing services, stealing data and/or money, child pornography, facilitating terrorist operations and disabling critical systems.

Sandhu explained that India's national cybersecurity policy, including the Joint Working Group on Public Private Partnership, provided a framework for a comprehensive, collaborative and collective response that would ensure a secure and resilient cyberspace for the government, businesses and citizens alike. The proposed Cyber Security Architecture would provide roles for different ministries to work together to create a secure online ecosystem that users could confidently navigate without fearing a cyber attack. A new initiative in the form of the National Cyber Coordination Centre aimed to monitor possible threats, provide early warnings to targeted sectors and trigger off responses to help limit the impact of attacks should they occur.

Building confidence in collaborative and collective responses to cyber attacks required strong public-private partnerships as well as a close working relationship between policymakers and academia. Training more people in cybersecurity and creating cybersecurity awareness through education to the public at large was also a way forward. Sandhu also noted the importance of international partnerships toward a more secure cyber arena.

John Yong discussed the growing complexity of the cyber threat landscape and Singapore's strategies to strengthen cybersecurity. He began his presentation underscoring the essentiality of information communication systems for businesses today and noted that Singapore, particularly with the many large financial institutions based within its borders, had long been known as a secure and trusted hub, implying how the country's continued economic viability hinged upon its ability to provide a secure place to do business.

In relation to the cyber threat landscape becoming more complex and multifaceted, Yong explained that threats could be both technical and non-technical in nature. He also said that the intentions behind various threats were different; while some might be linked to politics and ideology, others might be over attempts to make financial gains. To achieve their aims, cyber criminals had a range of means at their disposal such as disruption of service, defacement of websites and data theft. Cyber espionage was also a major additional concern for global companies and organisations, and such attacks could come not just from disparate individuals but from highly organised hacking groups and cyber vigilantes, even state-sponsored ones. Yong further said that there had been an explosion in the growth of new mobile malwares, and although that could be due to improvements in the ability to detect, collect and process malware, he emphasised that malware content remained difficult to uncover and could be hosted anywhere, including Singapore. Also posing a grave security challenge to identity protection and consumer data protection were the latest reiterations of phishing emails.

Moving on to Singapore's strategies for cybersecurity, Yong outlined the national-level information communication security programmes led and driven by the government. In particular, he focused on the Information Communication Security Masterplan 2 (MP2), a five-year plan that spanned 2008-2012, that had the objective of ensuring Singapore remained a secure hub. The plan was conceived to fundamentally address areas of concern such as emerging technologies, evolving threats, borderless cyber threats and ways to engender confidence. The strategic thrust of the plan was four-fold: (i) to harden national information communications infrastructure and services; (ii) to enhance information communications security competencies; (iii) to cultivate a vibrant information communications security ecosystem; and (iv) to increase international collaboration. In this regard, exchanging best practices in information security was crucial, and that included exploring international as well as public-private partnerships. Additionally, there was also the Cyber Watch Centre that provided round-the-clock security monitoring as well as preemptive alerts. As no organisation was a "lone island", Yong underscored the importance of the ability to identify and prioritise security through sound risk assessment and the capacity to recognise potential cascading impact of cybersecurity policies.

Paul Ducheine's presentation shed light on legal frameworks for cyber operations, with a particular focus on military cyber operations. He addressed issues related to the role of the armed forces in relation to cyber threats and cybersecurity, the varied conceptualisations of what constituted cyber warfare as well as the rules of engagement that could apply in such situations.

Ducheine set the environment of cyber operations in context by first explaining the meaning of cyberspace. Adopting the definition by the Dutch Advisory Council on International Affairs and Advisory Committee on Issues of Public International Law, cyberspace was regarded the man-made sphere that was "the sum of all ICT equipment and services… consist[ing] not only of the Internet but also of all the networks and other digital devices that are not connected to the Internet". Ducheine further discussed the sources of cyber threats as well as cybersecurity measures, with the latter, he said, encompassing a wide range of responses from both the government and the private sectors. Such responses included boosting cyber law enforcement, providing financial support or handing out penalties, and installing technical solutions.

Ducheine added that direct actions and disruptive operations could also be considered cybersecurity measures. Speaking specifically of military cybersecurity measures, he said such measures ranged from purely reactive actions to disruptive ones. The role and involvement of the military in cybersecurity, however, remained fairly limited, as most cybersecurity measures were private or civilian-led. The role of the Dutch armed forces in cyber operations, for instance, had to be juxtaposed against the constitutional task of the armed forces in national security as well as the country's vital interests. The legal framework necessitated that cyber operations conducted by the military fall into three main constitutional tasks: (i) defence; (ii) the promotion of the international legal order; and (iii) the protection of vital national interests, i.e. vital interests being interests that, if affected, could threaten the viability of society as a whole. With regard to cyber operations and cyber warfare, the military would undertake distinct roles in protection, intelligence, law enforcement, and constructive and disruptive operations. Additionally guiding military operations were the National Cyber Security Strategy as well as the Cyber Defence Strategy. Ducheine further explained the legal bases and legal regimes for cyber operations and the differences between them. Legal bases, for example, referred to the authority to conduct cyber operations whereas legal regimes could apply once operations had commenced. Ducheine highlighted the complexity of cyber operations by noting that any one cyber operation could be bounded by legal bases on the national level and multiple legal regimes at the international level, which included regulations on information communications technology, human rights and criminal laws.

NATO's Cyber Defence Policy

Christian-Marc Liflander, Policy Advisor, Cyber Defense Section, Emerging Security Challenges Division, NATO HQ

Christian-Marc Liflander focused his presentation on NATO's Cyber Defence Policy against the backdrop of NATO's Strategic Concept. Providing an overview of NATO and its approach to cybersecurity, he pointed out how NATO members abided by the principle of collective defence that recognised any attack against any one member as an attack against all. He added that NATO member states were presented with a unique opportunity platform to consult and discuss with one another regarding their respective security conceptions and that all NATO decisions were decided upon by consensus.

NATO, however, had not had cyber defence as part of its political agenda until the 2002 Prague Summit. The cyber defence agenda was subsequently built upon at the following summit in 2006. Further, it was not until the Estonia cyber attacks in 2007 that NATO was prompted to conduct a thorough assessment of its cyber defence policies. The Strategic Concept adopted at the Lisbon Summit in 2010 successively recognised that the development and use of destructive cyber tools could threaten unity and stability at both the national and Euro-Atlantic levels. It was at this point, Liflander noted, that there was a strategic shift in thinking about cyber defence.

Liflander went on to detail NATO's cyber defence policy. NATO's first priority was to protect its own networks and the primary vehicle through which to do so was through the NATO Computer Incidents Response Capability. The response team had the capacity to detect attacks when they occurred within NATO networks, spanning from the US to Afghanistan and beyond. It also provided software and hardware support and had advanced sensors that were placed at strategic points in NATO networks. These technologies comprised of elements such as e-mail monitoring, intrusion detection and security awareness. Liflander also highlighted that building cyber defence capabilities through the NATO Defence Planning Process was also of key strategic importance. By building capability targets for NATO members, each member state could focus on reaching their own goals. This was crucial as the NATO entity, being increasingly digitally interconnected, was only as strong as its weakest link, and the weakest state amongst them determined NATO's digital network overall strength, or its lack of.

As a way forward, Liflander identified training and education as essential elements in increasing NATO's cyber defence. The general public should not be disregarded in cyber defence; they needed to be actively engaged in order to foster a wider culture of online security. Public-private partnerships were also essential in ensuring a truly comprehensive cyber defence.

Liflander concluded his presentation by returning to the main theme of APPSNO 2013 which revolved around narrowing the theory and practice gap. He said theory and policy were inextricably linked and policymakers had to make sound decisions regarding the position of cybersecurity in the overall security agenda in conjunction with experts in the field of study.

Discussion

A participant enquired as to the challenges of engaging the private sector in cybersecurity and what could be done to incentivise the private sector in such a pursuit. A speaker responded by first reminding the audience that almost all the cybersecurity instruments currently available were owned by the private sector. It was thus of key importance that national security officers find appropriate ways to engage with the private sector. One of the foremost challenges was about being able to identify the right security product for the right organisation and that required an understanding not just of the security problems at hand but also of the existing technology available. Another speaker presented an example of good public-private engagement from the Netherlands where a Cyber Security Council had been established with both civil and private participations. The Council, co-chaired by a government official as well as the CEO of the country's leading internet service provider, had a dedicated research programme that gave out research grants to defence academies, universities as well as private companies. Another speaker from the panel quipped that every country needed to do individual assessments of their cybersecurity issues and come up with personalised solutions to the issue of public-private partnerships; such solutions could include handing out both incentives and disincentives to private businesses for cooperating in cyber defence issues.

Another participant asked how one could measure success in cybersecurity. In response, a speaker said that there would always be an amount of uncertainty in cyber defence in light of the fact that the real threats were really the ones nobody could actually see. There was no end state or victory in cyber defence as it was a constant process. That said, one way to evaluate the effectiveness of extant cybersecurity measures was to look at the amount of malware persistent within national networks as the extent of its presence indicated gaps in the security apparatus.

DISTINGUISHED LUNCH LECTURE
ADDRESSING COMPLEX NATIONAL SECURITY CHALLENGES – REFLECTIONS OF A SENIOR POLICYMAKER

Peter Ho

Setting his lecture in the context of a post-9/11 world, **Peter Ho** said that the first challenge to national security was the element of strategic surprise mainly in the form of 'black swans'. Black swans were rare, hard to predict, sudden and unique events with high impact that could lead to revolutionary turning points for existing trends or systems. They were, in other words, game changers. For example, the September 11 attacks changed the way people had to undergo security clearance at airports. Further, attempting to estimate the cumulative effects of black swan events was extremely difficult as made evident by the 2011 floods in Thailand which disrupted global supply chains across multiple industries, and the Arab Spring that led to the collapse of governments in Tunisia, Egypt, Libya and Yemen and brought about changes to the governments of Kuwait, Bahrain and Oman, even civil war in Syria.

Black swan events were inherently complex and would often defy replication or predictability. This was in contrast to complicated systems, which were designed to have replicable and reproducible effects. Defining complexity as the study of relationships between the system and the agents that acted within it, Ho explained that in such a setting the relationships and actions could give rise to collective behaviours that were not only unanticipated and not well understood, but could also deliver discontinuous and non-linear shocks to the system, resulting in catastrophic failure. He advised that it was thus necessary to be able to recognise that we were operating in a complex, not complicated, environment. In complex systems, policies would not solve all problems, and neither could it always be possible to get policies right the first time round.

The second challenge to national security was 'wicked problems'. These problems had highly complex causes and influencing factors that were not easily determined ex ante. As multiple stakeholders with different perspectives often had divergent goals, approaches to problem-solving and desired outcomes would be different and there would be no immediate or obvious solutions. Some examples of wicked problems were crowdsourcing, borderless criminal and terrorist cyber threats, human trafficking, smuggling, piracy, nuclear threats, climate change, food, water and energy security, water wars, demographic changes, and rapid urbanisation.

Further compounding the twin challenges of black swans and wicked problems was the fact that all human beings were prone to cognitive limitations that constrained our ability to deal with such complexities. Willful blindness, for instance, would make one deny the existence or probability of a threat; hyperbolic discounting would make one place more emphasis on immediate costs and benefits than on future risks and contingencies; and attention bias would make one focus just on one or two possible outcomes of a situation and ignore the rest. Policymakers would be additionally constrained by bounded rationality, a needed decision-making skill for making quick assessments under pressure with incomplete or limited information; they, therefore, could not make perfectly rational choices because the mind could not cope with the flood of information and demands that would come with black swans and wicked problems.

Nevertheless, Ho suggested that policymakers might learn to operate in a complex world through war-gaming or policy-gaming exercises that could help them overcome cognitive biases as they could contemplate thorny issues outside their comfort zones within a safe environment. He also recommended a whole-of-government approach to dealing with wicked problems. Additionally, there was a need to change mindsets to start engaging multiple stakeholders rather than focusing on just any one aspect of a particular problem. National needs should also take precedence over parochial interests.

Ho further made the suggestion for greater transparency and for policymakers to break down the vertical silos of departmentalisation. Policymakers should also operate on a knowing-enough basis through net assessments rather than a need-to-know basis, create structures to avoid group-think, identify threats through risk assessment and horizon scanning, and create lean, efficient and resilient organisations to cope with strategic shocks. Finally, to change mindsets towards 'whole-of-government' and 'whole-of-nation' perspectives, more seminars and courses targeted at mid- or senior level officers needed to be conducted to promote the sharing of experiences, for greater coordination between agencies, and to fight networked problems with a networked approach; APPSNO was a product of such an approach to addressing national security challenges.

Discussion

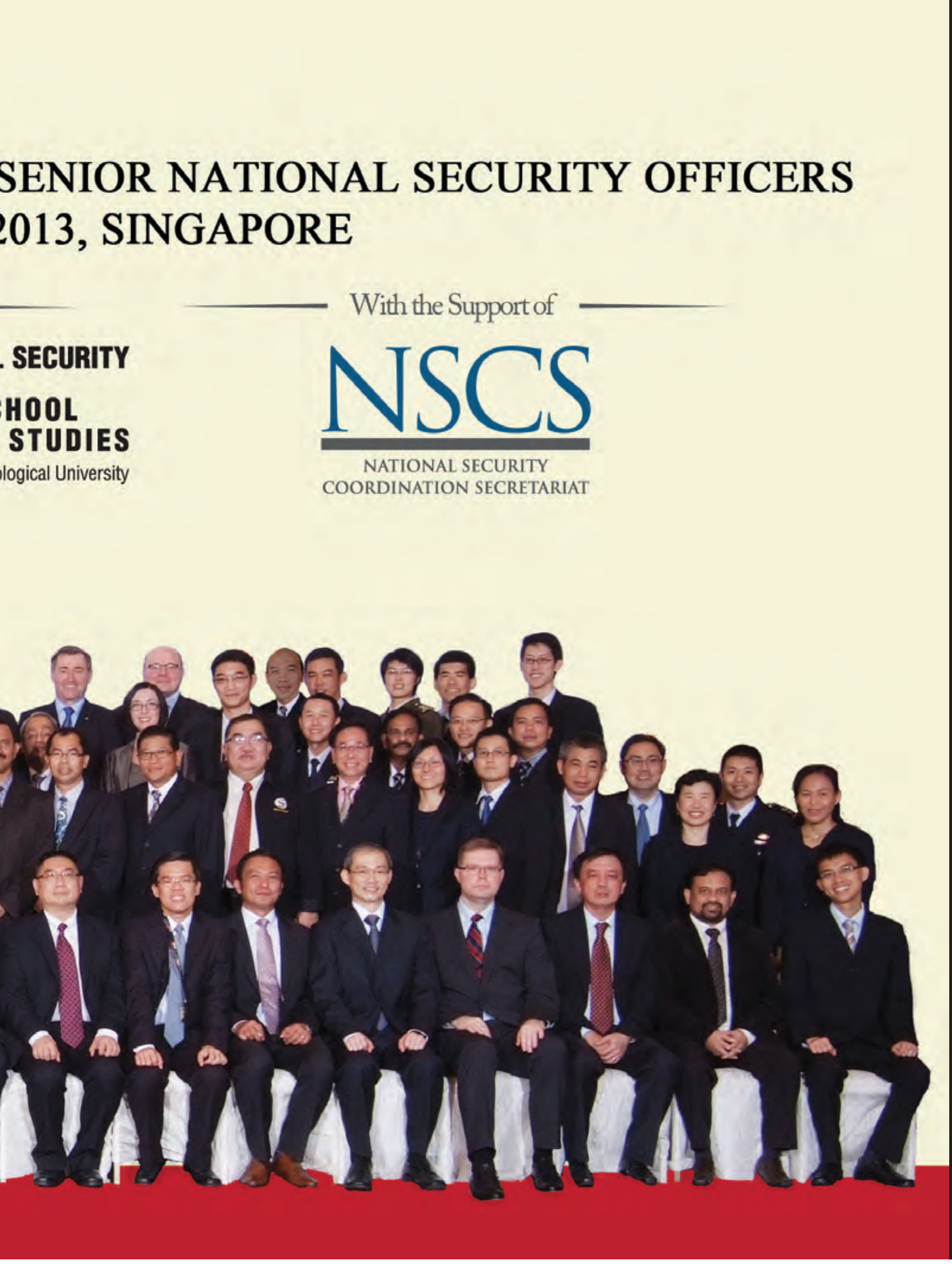
A participant asked how the government could work with the private sector to strengthen resilience in society. The speaker replied that it was important to not just think about a 'whole-of-government' but a 'whole-of-nation' approach to national security challenges. It was crucial to engage stakeholders who could define the problems and find the solutions. Just as important was to work with both the civil and private sectors to draw feedback and information regarding how policies might have impacted, for instance, private businesses and the economy. The NSCS, for example, held regular dialogues with the private sector and with people on the ground.

Another participant asked what could be done to increase international cooperation in fighting terrorism. The speaker understood that current conceptualisation of the terrorism threat was that terrorism was transnational in nature and not confined within the borders of a single country. JI, for instance, was regarded a pan-Southeast Asian threat. Terrorism could not be dealt with unilaterally, thus making international cooperation necessary. The speaker pointed out that there was actually very good international cooperation among intelligence agencies even if, at times, political relationships might not be ideal, underscoring the importance of forging professional relationships at the international level.

The final question was on whether cultural differences and changes could pose a security challenge. The speaker agreed that cultural differences would mean that one would look at the same issues from completely different perspectives with real impact on the dynamics on the ground. In relation to terrorism, for example, Europeans viewed the threat differently from the Americans. In Europe, people recognised that terrorism was a real problem but they learned to live with it as part and parcel of political life because they understood they could not throw in all of their resources to fighting it. In contrast, the Americans adopted an almost absolutist approach in countering terrorism. Culture, history and experience often shaped and informed such varied approaches. There was no single template for dealing with terrorism and it really could not be determined if one approach was right and the other wrong. That was why terrorism was a wicked problem.

APPSNO
2013
7TH ASIA-PACIFIC PROGRAMME FOR S
8 - 12 APRIL 2
Organised by
CENTRE OF EXCELLENCE FOR NATIONAL
S. RAJARATNAM SC
OF INTERNATIONAL
A Graduate School of Nanyang Techno
PONDER THE IMPROBABLE

CENTRE OF EXCELLENCE FOR NATIONAL SECU
S. RAJARATNAM SCHO
OF INTERNATIONAL ST
NSCS



International:

(Left-Right)

Seated : *Dr Damien D. Cheong, Dr Stefan Brem, Snr COL Xu Hui, COL Paul Ducheine, Mr Dmitri Trenin, Amb Richard LeBaron, Prof Joseph Liow, Assoc Prof Kumar Ramakrishna, PS (NSIC) Mr Benny Lim, Mr Eddie Teo, Amb Barry Desker, Mr Yeong Gah Hou, Mr Kok Ping Soon, Dr Norman Vasu, Mr Loh Kean Wah, Mr Christian-Marc Liflander, Mr John Yong, Mr Mohamed Feisal, Mr Wilber Lim*

2nd Row: *ME6 Yeo Heng Hwee, Supt Raja Sekaran M Vellu, AC Mohamed Farhad bin Mohamed Shariff, ME6 Kengadharan, Ms Christine June P. Cariño, Supt Sherrin Chua Yian Shing, Mr Ernest Soo, MG Ahmed Abdulaziz A Aleisa, Dr Abdullah M Bin Odah, Prof Irfan Idris, Police Col Khin Htay, Dr Chhuon Chanthan, MG B A Perera, Addl Insp Gen Md Nazmul Haque PPM, Mr Ahmad bin Haji Jaafar, Mr Ho Kong Wai, Supt Tan Kwang Seng, Mr Wong Siew Kwong, Ms Wong Siew Fong, Mr Yee Kwan Yew, Snr COL Tam Doan Van, Mr James Tan Kheng Koon, Ms Theodora Tan Peck Hiang, LTC Daniel Seet Siew Teck, Ms Lam Mong Teng*

3rd Row: *Supt Jarrod Pereira, Mr Ter Kwee Leng, Mdm Siew Chui Lin, Supt Christopher Lee Tuck Meng, Mr Erdem Mutaf, MG Ziauddin Najam, BG Jehad Matar, S/BG Abdulla Albaker, Dr Davaadorj Tseren, Amb Park Jae-Hyun, Mr Adrian Goh Soon Chye, Dr Bhashyam Kasturi, Ms Sophie Malone, Mr Ohm Cusripituck, SLTC Desmond Chong, ASP (APF) K Subramaniam, Mr Tony Hong Kian Chuan, Mr Seah Peng Leong*

4th Row: *Supt Ivan Goh Wee Khern, ME6 Jason Goh Puay Hiang, Mr Adam bin Haji Hamzah, Mr Chan Ee Pin Edwin, Mr Rob Duiven, Mr Lee Cheow Hiang, Mr Jeremy Ng Hin Kay, Mr Dominic John Baptist, SLTC Leong Chun Siu, Dr Michael Ong Chin Cheong, Gen Franz Lang, Dr Matti Saarelainen, Mr Chin Ming Kang, Mr Kwan Chee Keong, LTC Karen Wong Poh Fern, Mr Tan Peng Soon, Mr Jonathan Ng Wen Hao*

DISTINGUISHED DINNER LECTURE

ADDRESSING THE NATIONAL SECURITY CHALLENGES OF THE 21st CENTURY: THE NEED FOR BETTER ACADEMIC-PRACTITIONER COLLABORATION

Robert Hutchings

In his lecture, **Robert Hutchings** observed a widening gap between the worlds of policy and of learning in the US and in many other countries at a time when the need for the two worlds to come together could not be greater considering the challenges of the day. He suggested three ways to close the gap, by: (i) making the academic disciplines more relevant, (ii) making policy makers more accessible, and (iii) developing global partnerships for the study and practice of diplomacy.

Hutchings noted that the world was in the midst of the most profound global power shifts in over a century. The collapse of the Cold War order, the rise of China and India as global powers, and the advent of new transnational challenges had all combined to overturn old verities and points of references.

In light of the aforementioned global issues, the disjuncture between academics and policy practitioners presented challenges to problem solving. Hutchings observed that academics tended to be comfortable with theorising and forecasting ongoing issues. Meanwhile, policymakers tended to concentrate on contingencies and were at times adamant that changes could not be viewed through the lens of arithmetic and models. Hutchings saw that governments tended to be weak at long-term planning largely because their attention tended to be focused on dealing with more immediate demands, and because of the unpredictable nature of change, strategic thinking tended to take the backseat in policymaking.

To narrow the academic-policy gap, Hutchings suggested that governments improve diplomatic education and training. He believed that diplomacy should play a greater role in contemporary national security. Current diplomatic training mainly aimed to provide practical knowledge and know-hows for those in the diplomatic vocation, but Hutchings asserted there was potential in taking diplomatic training further than what it was in its current state. He saw, for instance, value in in-depth historical research into the practice of diplomacy in order to frame issues more accurately. Also, he believed there was a need to create strategic planning capacities as well as a culture of openness and accessibility among the government institutions. Further, those in academia needed to look beyond theories and make their work more relevant to policy issues.

Discussion

A topic discussed was regarding the role of multilateral institutions such as the Association of Southeast Asian Nations (ASEAN) and the Asia-Pacific Economic Cooperation (APEC) in national security. It was noted that multilateral institutions in Europe had a long history of contributing to the resolution of national security issues. However, there might be a need to reassess the current hierarchy of multilateral institutions to reflect the new global balance of power.

Also discussed were the rise and fall of great powers and the evolving relationships among the global players. Historically, the rise of a new power usually resulted in one form of disruption or another. Revisionist powers would often seek to carve out new places for themselves in the international system commensurate with their new powers whilst the great powers would typically resist rising ones. Such dynamism would have impact on international relations.

The question of whether extant political systems could continue was also posed. Political pluralism that allowed for more voices to be heard within the system was forwarded as one of the best ways for emerging powers to continue in their rise. In a world where political change could be driven by bloggers in cyberspace, it would be counterproductive, particularly for some rising powers, to attempt to control the change as it could adversely affect their desire to get ahead.

SESSION V
COUNTERING VIOLENT EXTREMISM AND RADICALISATION

Opening Address by Mr Teo Chee Hean
Prime Minister, Coordinating Minister for National Security and Minister for H

(from left) Kumar Ramakrishna, Muhammad Tito Karnavian, Bilveer Singh, Mohamed Feisal bin Mohamed Hassan and Abdulrahman AlHadlaq

Kumar Ramakrishna developed the concept of the "Manichean Mindset" from theories in psychology to examine how individuals could be radicalised into violent extremism. He posited that the Manichean Mindset was a default human instinctual setting derived from the unconscious tribal impulse to defend one's in-group identity or "Group Tent". Its four elements were the tendency to see the world in binary terms, the perception of the in-group as the centre of one's social universe, a distrust of out-groups, and the desire for one's Group Tent to be higher in the social pecking order than the out-groups'.

Violent extremism might occur when members of an in-group perceive their Group Tent to be under serious threat of sociopolitical marginalisation or extinction, resulting in an acute identity simplification process. Cognitive radicalisation occured when the multiple identities within a stressed community were drastically simplified to a single overarching "Us" in-group while the other community was likewise reduced to a single overarching adversarial "Them" out-group. However, while cognitive radicals might be alienated and harboured grievances, they might not necessarily turn violent.

The challenge accordingly lay with cognitive extremists who would positively accept violence in politics, which might in turn lead to terrorism and genocide owing to an amplified Manichean Mindset. Such individuals were often fanatically closed-minded, accepted democratic processes only as a stairway to power, were supremacist, authoritarian, intolerant and dogmatic in outlook, rejected equality, diversity and human rights, and embraced the use of political violence.

Ramakrishna identified four supporting factors in the transition to violent cognitive extremism: (i) a collectivist hierarchical culture that emphasised obedience to authority; (ii) an ideology that consciously justified violence in pursuit of religious or political goals; (iii) a small group dynamic led by charismatic leaders in a cult-like atmosphere that maintained physical and psychological isolation from alternative ideas; and (iv) an enabling environment such as social and economic deficits and poor life prospects, weak law and order, and access to weapons.

Ramakrishna concluded that effective measures to counter violent extremism should not only focus on counter-ideological programs and law enforcement but also on preventing the innate Manichean Mindsets from radicalising into cognitive extremism through a deliberate process of personalising, de-categorising and humanising out-groups.

Mohamed Feisal Bin Mohamed Hassan shared the experience of the Religious Rehabilitation Group (RRG) in Singapore – a voluntary group of religious scholars working with psychologists, case officers, researchers and community groups in the rehabilitation of Jemaah Islamiyah (JI) detainees – in winning the hearts and minds of radicals and extremists and inoculating the community from radicalisation.

A key pillar of the work of the RRG was religious counseling for the JI detainees, an endeavour that involved extricating negatively imbibed ideology, replacing negative ideology with positive ones, imbuing a rightful understanding of Islamic knowledge and exemplifying fulfilling ways of living in a multi-racial, multi-religious society. Beyond the focus on detainees, the RRG also offered community support to their families. Additionally, the RRG conducted public outreach programmes such as dialogue sessions, talks and conventions that addressed issues of religious extremism, the promotion of moderation, and an appreciation of living in a multi-racial and multi-religious environment. These programmes drew on academic insights garnered through the Group's partnerships with various academic institutes such as the S. Rajaratnam School of International Studies (RSIS).

Mohamed then highlighted five challenges facing the RRG: the phenomenon of self-radicalised individuals, the harnessing of social networks by radical groups, the proliferation of radical internet ideologues, and the broadening of radical propaganda to reach out to English-speaking audiences.

Muhammad Tito Karnavian assessed the successes and challenges faced by Indonesia's Detachment 88 (D88) when employing academic approaches to counterterrorism. D88 was established in 2003 as a special police unit for countering terrorism in Indonesia following the wave of terrorist incidences in Indonesia between 2000 and 2002. Recognising that tactical law enforcement operations alone were insufficient to contain the terrorist threat, the unit developed a broader understanding of terrorism to neutralise the complex threat more effectively.

Following from this, officers were not just provided professional but international academic training too. Academic lenses and methods were employed to assess terrorist groups, new trends in terrorism and best practices in counterterrorism strategies in Indonesia and beyond, leading to the development of a strategic and operations framework grounded in a law-enforcement approach. Other measures informed by academia included the adoption of soft measures in engaging radical individuals and the wider community, developing systematic approaches to neutralising recruiters and stemming the radical ideology, and understanding the underlying causes of terrorism.

Tito highlighted three ways in which applying the academic lens to counterterrorism in Indonesia contributed successfully to counterterrorism efforts on the ground. Firstly, it provided the officers with a deeper and more comprehensive understanding of the terrorism phenomena. Secondly, the more rigourous analysis of data was instrumental in the development of better strategies and operations. Thirdly, a wide range of academic perspectives on terrorism helped the unit appreciate the complexity of the phenomenon of terrorism, resulting in the push for the need of an interagency approach as well as the implementation of soft approaches to win the hearts and minds of the wider public. Tito also identified some challenges of this approach namely determining the relevant/appropriate methodologies and best practices to adopt, and the imperative for better collaboration between academics and practitioners.

Abdulrahman AlHadlaq presented on Saudi counter-radicalisation efforts. The Saudis adopted a "3M theory" to identify the main factors leading to terrorist recruitment in Saudi Arabia. The first 'M' referred to men with grievances and organisational capacity; such individuals with radical mindsets were deemed most likely to gravitate towards terrorism. The second 'M' referred to money channeled to terrorist organisations; to address this issue, Saudi Arabia established control mechanisms, including the Financial Investigating Unit (FIU), a specialised department to regulate the movement of finances to thwart financial support for terrorist activities. The third 'M' referred to the mindset of extremists harbouring violent ideology, which was the greatest of the three 'M's to address.

AlHadlaq went on to elaborate on the Saudi strategy of Prevention, Rehabilitation and After-Care (PRAC) to counter radicalisation and extremism. PRAC comprised three interconnected programmes aimed at discouraging individuals from potential involvement in extremism, promoting the rehabilitation of extremists, their supporters and sympathisers, and providing aftercare programmes to facilitate the reintegration of extremist detainees released into Saudi society after their release from custody.

The first programme focused on preventing the spread of radical violent ideology. Efforts to this end involved rectifying misunderstandings about Islam as well as the propagation of moderate Islam through various media outlets and engagement with religious institutions, educational institutes and civil society.

The second programme provided rehabilitative counseling and care with the goal of replacing the extremist ideology of detainees with that of a moderate one and to prepare them for reintegration into Saudi society after their release. Support was not only provided for the detainees but their families too in order to win over their hearts and minds to curtail the recruitment pool of potential terrorists. While rehabilitative counseling was provided in prisons for the detainees, preventive counseling was also carried out outside of prisons targeting vulnerable places, families and lines of communication.

The third programme was the after-release care programme. It involved keeping in touch with the released detainees and their families, facilitating their reintegration into society through the continuation of financial and moral support, equipping them with the necessary skills to gain employment or further their studies, and assisting them in starting families where necessary.

Drawing lessons from the Saudi experience, AlHadlaq concluded that comprehensive strategies, adequate resources, sound programmes and evaluation processes, and international cooperation were crucial to counter radicalisation.

Discussion

A key issue debated pertained to the distinction between peaceful and violent extremists and radicals and the speakers had varied takes on it. One argued that an important factor was an individual's ability to deal with ambiguity; unlike radicals who could still be reasoned with, extremists were more likely to have a rigid binary worldview and were thus more vulnerable to violent ideologies and were also more difficult to reintegrate into mainstream society. Another speaker added that the concept of a peaceful radical or extremist was relative. Some groups, such as the Muslim Brotherhood, might be considered peaceful by some but not so by others. Since there was no consensus on what constituted 'moderate' religious practices, those who observed religious customs and practices that were deemed extreme by others could be considered peaceful extremists if they did not enforce their beliefs on others. Another speaker, drawing references from the Indonesian context, emphasised that those considered extremists and fundamentalists might not necessarily be violent. For instance, Islamist groups whose goal was to establish an Islamic state in Indonesia could be divided into militant groups who used violence and non-militant groups who employed non-violent means. A member of the audience further contributed that terrorists who killed in the name of Islam should not be referred to as "Islamist terrorists", which would suggest that they were worthy of being considered Muslims, but merely terrorists who abused Islam.

On the question of measures taken to reintegrate Singapore's JI detainees with the wider non-Muslim community, it was explained that a key effort of the RRG was to ensure that the public was aware of the reality and challenges posed by JI to Singapore. Of note was the Group's effort to dispel any misinterpretation of Islamic teachings, especially those harboured by the detainees, through various platforms of public engagement.

PROGRAMME

SUNDAY, 7th APRIL 2013

0001 – 2359hrs **Arrival of Speakers & Participants**
Venue:
The Sentosa, A Beaufort Hotel,
Singapore

1500 – 1730hrs **Registration of Speakers & Participants**
Venue:
Conference Secretariat
Kusu Room, The Sentosa,
A Beaufort Hotel, Singapore

1830 – 2100hrs **Welcome Dinner**
Hosted by:
Barry Desker, Dean, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU)

Kok Ping Soon, Senior Director, National Security Coordination Centre (NSCC), Prime Minister's Office, Singapore

Venue:
Poolside, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Casual (short-sleeved shirt/polo t-shirt) and equivalent attire for women

MONDAY, 8th APRIL 2013

0730 – 0830hrs **Breakfast**
Venue:
The Terrace Restaurant, The Sentosa,
A Beaufort Hotel, Singapore

0830 – 0915hrs **Arrival of guests**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

0915hrs **All guests to be seated**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

0920hrs **Arrival of Guest-of-Honour**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

0930 – 0940hrs **Opening Remarks**
Barry Desker, Dean, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore

Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

0940 – 1000hrs **Opening Address**
Teo Chee Hean, Deputy Prime Minister, Coordinating Minister for National Security and Minister for Home Affairs, Singapore

Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

1000 – 1030hrs **Reception / Coffee Break**
Venue:
Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

1030 – 1115hrs **Group Photo-taking**
Venue:
Beaufort Ballroom I, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

1115 – 1130hrs **Local Participants Briefing**
Briefing by **Loh Kean Wah**,
Deputy Director (Policy & International Relations), National Security Coordination Centre, Prime Minister's Office, Singapore

Venue:
Beaufort Ballroom I, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Military attire/service dress (jacket with tie and head-dress) for officers; lounge suit with tie for civilians and equivalent attire for women

1130 – 1145hrs **Introduction to RSIS, CENS and APPSNO**
Presenter:
Kumar Ramakrishna, Head, Centre of Excellence for National Security (CENS), RSIS, NTU

Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1200 – 1315hrs **Lunch**
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1315 – 1400hrs **Session I:**
Singapore's Strategic Framework for National Security
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speaker:
Kok Ping Soon, Senior Director, National Security Coordination Centre (NSCC), Prime Minister's Office, Singapore

Question and Answer Session

1400 – 1415hrs **Coffee Break**
Venue:
Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1415 – 1420hrs **Assemble for Heritage Walk**
Venue:
Meet at the Main Lobby of The Sentosa, A Beaufort Hotel, Singapore

Attire:
Casual (APPSNO T-shirt) and equivalent attire for women.
No shorts and slippers

1420 – 1900hrs "**In Search of the Singha™" - A Fort Canning Hill / Singapore River Walk + Bum Boat Ride**
Attire:
Casual (APPSNO T-shirt) and equivalent attire for women.
No shorts and slippers

1900 – 2100hrs **Networking Dinner**
Venue:
AquaMarine, Marina Mandarin Hotel

Attire:
Casual (APPSNO T-Shirt) and equivalent attire for women.
No shorts and slippers

TUESDAY, 9th APRIL 2013

0730 – 0900hrs **Breakfast**
Venue:
The Terrace Restaurant, The Sentosa,
A Beaufort Hotel, Singapore

0900 – 1030hrs **Foreign Participants' Presentation on Homeland Security Management (HSM)**
(Australia/ Austria/ Bangladesh/ Brunei/ Cambodia/ China/ Finland & India)
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1030 – 1045hrs **Coffee Break**
Venue:
Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie)

1045 – 1215hrs **Session II:**
National Risk Assessment and Management: Insights from the US, UK, and Switzerland
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Chairperson:
Kok Ping Soon, Senior Director, National Security Coordination Centre (NSCC), Prime Minister's Office, Singapore

Speakers:
Alan D. Cohn, Assistant Secretary for Strategy, Planning, Analysis & Risk, DHS. Office of Policy, USA

John Tesh, Visiting Senior Fellow, Department of War Studies King's College, London; Former Deputy Director, Civil Contingencies Secretariat UK Cabinet Office, UK

Stefan Brem, Head, Risk Analysis and Research Coordination, Federal Office for Civil Protection, Switzerland

Question and Answer Session

Lunch Lecture

1215 – 1300hrs **Lecture:**
Emergent Issues in Asian Food Security
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speaker:
Paul Teng, Dean, Graduate Studies and Professional Learning, National Institute of Education; Senior Fellow (Food Security), Centre for Non-Traditional Security (NTS) Studies, RSIS, NTU, Singapore

Question and Answer Session

1300 - 1400 **Lunch**:
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1400 – 1730hrs **Perspectivity Game**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Facilitators:
Perspectivity Foundation

1730 – 1930hrs **Free and Easy**
3rd APPSNO Alumni Dinner Lecture

1830 – 1930hrs **Cocktail Reception**
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1930 – 2010hrs **Lecture:**
Leadership in National Security: Applying Operational Lessons
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speaker:
Bernard Miranda, Director, National Maritime Operations Group, National Maritime Security System, Singapore

Question and Answer Session

2010 – 2130hrs **Dinner**
Venue:
The Beaufort Ballroom, The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

WEDNESDAY, 10th APRIL 2013

0730 – 0900hrs **Breakfast**
Venue:
The Terrace Restaurant, The Sentosa, A Beaufort Hotel, Singapore

0850 – 0900hrs **Assemble for Travel to Home Team Academy**
Venue:
Conference Lobby of The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

0900 – 1000hrs **Travel to Home Team Academy (HTA)**

1000 – 1200hrs **Session III:**
Strategic and Crisis Communication
Venue:
Home Team Academy

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Chairperson:
Yolanda Chin, Research Fellow & Coordinator of Social Resilience Programme, Centre of Excellence for National Security (CENS), RSIS, NTU

Speakers:
Richard LeBaron, Visiting Senior Fellow, The Rafik Hariri Centre for the Middle East, Atlantic Council, USA

Xu Hui, Professor and Deputy Commandant for Academics, College of Defense Studies, National Defense University, People's Liberation Army, China

Philip Sim, Deputy Director, Emergency Preparedness Office, Public Communications Division, Ministry of Communications and Information, Singapore

Dmitri Trenin, Director, Carnegie Moscow Centre, Russia

Question and Answer Session

1200 – 1330hrs **Lunch**
Venue:
Home Team Academy

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1330 – 1530hrs **Tour around Home Team Academy (HTA)**

1530 – 1630hrs **Return to Hotel**

1630hrs **Free and Easy**

THURSDAY, 11th APRIL 2013

0730 – 0900hrs **Breakfast**
Venue:
The Terrace Restaurant, The Sentosa,
A Beaufort Hotel, Singapore

0900 – 1030hrs **Foreign Participants' Presentation on Homeland Security Management (HSM)**
(Indonesia/ Jordan/ Malaysia/ Mongolia/ Myanmar/ Netherlands & Pakistan)
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1030 – 1045hrs **Coffee Break**
Venue:
Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie)

1045 – 1225hrs **Session IV: Cybersecurity**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speakers:
Nehchal Sandhu, Deputy National Security Advisor, National Security Council Secretariat, India

John Yong, Director, Infocomm Security & Assurance, Infocomm Development Authority of Singapore

Paul Ducheine, Associate Professor of Cyber Operations and Cyber Security, Netherlands Defence Academy, University of Amsterdam, The Netherlands

Christian-Marc Liflander, Policy Advisor, Cyber Defense Section, Emerging Security Challenges Division, NATO HQ

Question and Answer Session

1225 – 1310hrs **Distinguished Lunch Lecture**
Lecture:
Addressing Complex National Security Challenges – Reflections of a Senior Policymaker
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speaker:
Peter Ho, Chairman, Urban Redevelopment Authority Board; Senior Advisor, Centre for Strategic Futures; Senior Fellow, Civil Service College; Adjunct Professor, RSIS, NTU, Singapore

Question and Answer Session

1310 - 1410 **Lunch**
Venue:
The Beaufort Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1425 – 1525hrs **Syndicate Discussions**
Syndicate 1
Venue:
The Straits Ballroom, The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Syndicate 2
Venue:
Beaufort I, The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Syndicate 3
Venue:
Beaufort II, The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1525 – 1540hrs **Coffee Break**
Venue:
Straits Verandah, The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1540 – 1700hrs **Free and Easy**

1700hrs **Travel to Asian Civilisations Museum**
Venue:
Meet at the Conference Lobby of The Sentosa, A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Distinguished Dinner Lecture
1730 – 1830hrs **Cocktail Reception**
Venue:
Asian Civilisations Museum

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1830 – 1915hrs **Lecture:**
Addressing the National Security Challenges of the 21st Century: The Need for Better Academic – Practitioner Collaboration
Venue:
Asian Civilisations Museum

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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

Speaker:
Robert Hutchings, Dean, Lyndon B. Johnson School of Public Affairs, University of Texas, USA

Question and Answer Session

1915 – 2130hrs **Dinner**
Venue:
Asian Civilisations Museum

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

FRIDAY, 12th APRIL 2013

0730 – 0900hrs **Breakfast**
Venue:
The Terrace Restaurant, The Sentosa,
A Beaufort Hotel, Singapore

0900 – 1030hrs **Foreign Participants' Presentation on Homeland Security Management (HSM)**
(Philippines/ Qatar/ Saudi Arabia/ South Korea/ Sri Lanka/ Thailand/ Turkey & Vietnam)
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1030 – 1045hrs **Coffee Break**
Venue:
Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1045 – 1245hrs **Session V:**
Countering Violent Extremism and Radicalisation
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Chairperson:
Bilveer Singh, Associate Professor, Department of Political Science, National University of Singapore; Adjunct Senior Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU

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

Mohamed Feisal Bin Mohamed Hassan, Associate Research Fellow, International Centre for Political Violence and Terrorism Research, RSIS, NTU, Singapore

Tito Karnavian, Chief of Police, Papua Province, Indonesia

Abdulrahman AlHadlaq, Director General, Ideological Security Directorate, Ministry of Interior, Kingdom of Saudi Arabia

Question and Answer Session

1245 – 1300hrs **Course Evaluation**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1300 - 1430 **Lunch**
Venue:
The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:
Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1430 – 1530hrs **Syndicate Discussions**

Syndicate 1

Venue:

The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Syndicate 2

Venue:

Beaufort I, The Sentosa, A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Syndicate 3

Venue:

Beaufort II, The Sentosa, A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1530 – 1600hrs **Coffee Break**

Venue:

Straits Verandah, The Sentosa,
A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1600 – 1800hrs **Free and Easy**

Certificate Presentation Ceremony and Closing Dinner

1800 – 1900hrs **Cocktail Reception**

Venue:

The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

1900 – 2130hrs **Certificate Presentation Ceremony and Closing Dinner**

Hosted by:

Benny Lim, Permanent Secretary, National Security and Intelligence Coordination, Singapore

Venue:

The Straits Ballroom, The Sentosa,
A Beaufort Hotel, Singapore

Attire:

Smart casual (long-sleeved shirt without tie) and equivalent attire for women

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, cybersecurity 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