11TH ASIA-PACIFIC PROGRAMME FOR SENIOR NATIONAL SECURITY OFFICERS: INNOVATION AND NATIONAL SECURITY

Event Report
3-7 April 2017

Centre of Excellence
for National Security

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

NSCS NATIONAL SECURITY COORDINATION SECRETARIAT

Event Report

11TH ASIA-PACIFIC PROGRAMME FOR SENIOR NATIONAL SECURITY OFFICERS (APPSNO)

3-7 April 2017
Singapore

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

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

Rapporteurs:
Muhammad Faizal bin Abdul Rahman, Juhi Ahuja, Nur Diyanah binte Anwar, Joseph Franco, Cameron Sumpter, Dymples Leong Suying, Pravin Prakash, Romain Brian Quivooij, Tan E Guang Eugene, and Jennifer Yang Hui

Editors:
Benjamin Ang, Damien D Cheong, and Norman Vasu

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The 11th Asia-Pacific Programme for Senior National Security Officers (APPSNO) was held at Marina Mandarin Singapore from 3 – 7 April 2017. Organised by the Centre of Excellence for National Security (CENS) with the support of the National Security Coordination Secretariat (NSCS) in the Prime Minister's Office (PMO), APPSNO 2017's theme was "Innovation and National Security".

Speakers from a wide range of countries such as Australia, Czech Republic, Latvia, The Netherlands, Philippines, Singapore, the United Kingdom and the United States, shared their expertise and experience on these topics:

1. **Innovation and Technology** – cyber threats to smart cities, machine learning, and the future of big data in cybersecurity

2. **Resilience in the Post-Truth Era** – the divisive impact of fake news, influence operations and information warfare, and new ways of responding

3. **Innovation in Terrorism and Counter-terrorism** – community led intervention, tools for assessing violent extremism

4. **Innovation in Strategic Communication** – new methods for internal and external communications in crises, changes in social media and communications landscape

5. **Case Studies** – artificial intelligence, the role of hackers in national security

The event brought together senior national security officers from the Asia Pacific and beyond to Singapore for a week of intensive discussion and networking. More than 70 participants from over 21 countries met to discuss the challenges of national security. Foreign participants were joined by their Singaporean counterparts from various government ministries and agencies. In keeping with the theme of innovation, guest of honour, Mr K Shanmugam, Minister for Home Affairs and Minister for Law, conducted a closed-door dialogue session that was restricted to the foreign and local participants of the conference.

Besides listening to panel presentations and engaging in small group discussions with the speakers, foreign participants gave country presentations, which provided a concise overview of their respective states'

policies and challenges to national security. Further enriching the programme was a distinguished alumni dinner lecture by Mr Peter Ho on the importance of innovation in national security, and a distinguished lecture by Mr Chris Kirchhoff, US Department of Defence, on innovation in defence. Overall, there was a broad consensus among speakers and participants alike that APPSNO was an interesting, insightful and valuable event.

Session 1: Innovation and Technology

The Challenge of the 21st Century—Embedding Safety and Security in a New World of Smart Cities
Simon Moores, Director of Research, Zentelligence (Airads) Ltd, United Kingdom

The emergence of and growing complexity of smart cities require a rethinking of how to embed trust in the technological systems they are based on, to ensure both security and privacy of individuals.

Managing Multi-way Cyber Insecurity Dilemmas in Asia
John C Mallery, Research Scientist, Computer Science & Artificial Intelligence Library, Massachusetts Institute of Technology, United States

The ongoing cyber arms race contributes to the destabilisation of international security. This destabilisation can only be resolved with greater international collaboration.

Singapore's Cybersecurity Strategy – Not Just Technology
Benjamin Ang, Senior Fellow and Coordinator, Cyber Programme, Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

The foundation of Singapore's national Cybersecurity Strategy is based on harnessing the benefits of technological advancement coupled with an investment in human capital.

Distillation

1. Further comparative analysis is needed to identify common themes between cities aiming for smart city status. This can help ensure a comprehensive whole-of-nation approach towards achieving the Smart Nation goal.

2. Policies are needed to increase awareness of decision-makers to cybersecurity threats facing the Smart Nation.

3. There is a need to carefully evaluate what services should be considered critical cyber infrastructures in a Smart Nation, so that appropriates policies and measures can be taken to protect them.

4. The range of critical infrastructure vulnerable to cyber-attack has evolved to include non-physical assets such as electoral processes.

5. Emerging global norms should take into consideration the growth of cyber insecurity, the intensification of asymmetric conflicts, and the blurring lines between civilian and military targets, because existing norms that cover conventional warfare and state-level conflict may be inadequate at present.

Session 2: Resilience in the Post-Truth Era

The Weakest Link to Resilience: Establishing a Credible Reputation Defence in a Post-Truth Era
Ryan Lim, Founding Partner; Principal Consultant, QED Consulting Pte Ltd., Singapore

Hoaxes, disinformation and fake news are very much a part of daily life today. They can be weaponised and turned into a threat against social stability and harmony.

Russian Influence and Disinformation Operations in Europe
Jakub Janda, Head, Kremlin Watch Programme, Deputy Director for Public Policy, European values Think-Tank, Czech Republic

Targeted disinformation campaigns often attack the official / state narrative rather than individual targets, in order to promote counter narratives that can destabilise public consensus and social cohesion.

Integrating Resilience in Defence Planning against Information Warfare
Janis Berzins, Director, Centre for Security and Strategic Research, National Defense Academy of Latvia, Latvia.

Sources of disinformation can range from Non-Governmental Organisations (NGOs) to elected officials, within the targeted state, whose political agenda aligns with the disinformation campaign. The strategy is one of direct attack to foster inner decay.

Distillation

1. There is an urgent need to build resilience against disinformation and fake news. Such a strategy must be non-invasive, non-aggressive, and will take time.

2. Building this resilience will require constant vigilance and monitoring of the information environment as well as the ability to operationalise resilience by measurable criteria.

3. Resilience building will also require a wide range of policies. This includes targeting the cognitive capacity of the polity by equipping them with the skills necessary to recognise hoaxes and fake news, as well as effective policies and effective strategic communications that convey accurate information to the people and win both hearts and minds.

4. The private sector may be an effective resource from which states can learn how to build effective strategic communications strategies as well as how to build effective resilience against disinformation.

Session 3: Innovation in Terrorism and Counter-Terrorism

Developments in Counter-Terrorism
Ali Soufan, Chairman and Chief Executive Officer, The Soufan Group, United States

The international community has been focused on the Islamic State (IS), but Al-Qaeda (AQ) has also grown in strength. Countering the enduring ideology of Jihadist groups needs to be considered a top priority.

Re-examining solutions to Countering Violent Extremism: building effective community-led interventions
Clarke Jones, Australian Intervention Support Hub (AISH)

Working with families and communities is a key element of programmes aiming at countering violent extremism (CVE). Approaches exclusively focusing on intelligence and law enforcement are counter-productive.

Risk Assessment for Violent Political Extremism: National Security Applications
Elaine Pressman, Netherlands Institute of Forensic Psychiatry and Psychology

The threats of radicalisation and violent extremism have made risk assessment a key national security tool. Structured professional judgment, based upon human analysts and formalised protocols, is the most accurate risk assessment metric.

Distillation

1. The threat landscape has changed with the professionalisation of online Jihadist propaganda and the increasingly dominant role of so-called "lone wolves" in the preparation and the execution of terror attacks. These individuals increase the pressure on intelligence and law enforcement agencies as the gap between radicalisation and mobilisation is shortened.

2. Expressions such as "radicalisation", "deradicalisation" and "countering violent extremism" can be perceived as offensive by some individuals and communities. CVE practitioners should be flexible and figure out different engagement approaches. Another flaw is for authorities to favour top-down and risk-based approaches that consider individuals as threats.

3. Informal risk assessment approaches only based on subjective elements, such as the intuition and experience of analysts, are limited. Structured professional judgment (SPJ) is arguably the best approach. Analysts are tasked with assessing a structured protocol containing a large volume of data and interpreting the information contain therein. The value of the SPJ is the ability to combine scientific methods of data collection with professional judgment.

Session 4: Innovation in Strategic Communication

Multi-Platform (UAV, UGV, and Mobile User) Information and Communications Systems for Disaster Risk Reduction
Gregory Tangonan, Professor, Founding Director, Ateneo Innovation Center, School of Engineering, Ateneo de Manila University

International cooperation and information sharing is important for disaster management. Currently the Philippines is partnering with advocates in Japan and Southeast Asia to make V-Hub technology the new Asian standard for disaster communications

The Role of Media Literacy in Combating Fake News
Lock Wai Han, Chairman, Media Literacy Council; Chief Executive Officer, OKH Global Ltd.

While public education and instilling corporate responsibility are important, the responsibility for critically evaluating online sources ultimately rests with the individual. Therefore, future Media Literacy Council (MLC) campaigns should aim to bolster digital maturity in individuals.

Challenges in the Social Media and Communications Landscape
Alvin Tan, Head of Public Policy, South East Asia, Facebook

To address the challenges of hate speech and online radicalisation, cooperation that incorporates a wide spectrum of expertise to inform policies is necessary. In the future, Facebook seeks to engage credible voices from different age groups and religious backgrounds to assist its quest against online violent extremism.

Distillation

1. Disaster/ emergency response should look into understanding the community's social connectivity before an incident takes place.

2. Further research is needed to find out how to help individuals critically evaluate online materials.

3. The private and public sector must work more closely with each other to tackle violent extremism online.

Session 5: Case Studies

Climate Change, Disaster Risk and Scientific Tools: Philippines Case Study
Antonio Yulo Loyzaga, Chairperson, International Advisory Board, Manila Observatory

Disaster and risk management form a critical branch of the Philippines' national security strategy. Innovative scientific research and creative responses are required to address environmental pressures brought about by climate change, increased human activity, and urbanisation.

Hackers Lead the Way
Jeff Moss, Founder and CEO of Def Com Communications and the Black Hat Briefings

Hackers have become broadly viewed as mischievous societal outliers and subversive criminals. Governments should instead appreciate their unique skill-sets and motivate them to protect national information security.

National Security Implications of the Fourth Industrial Revolution
Linton Wells, President and Chief Executive Officer, Global Resilience Strategies

The Fourth Industrial Revolution is significantly disrupting global human activity in areas such as governance and labour markets. Radical changes to processes and societal organisation will be required to manage the unprecedented velocity of technological developments.

Distillation

1. Investment in environmental science research and innovative responses to disaster management are critical in the emerging era of increasingly frequent and severe weather events brought about by climate change.

2. Governments need to embrace the inherent curiosity and technical skill of young hackers who are often at risk of falling into criminal behaviour because of sanctions derived from counterproductive policies and disproportionately harsh legislation.

3. Global technological advancement, rapidly increasing complexity, and the fusing of biological and digital phenomena have such disruptive potential that entire societies may need to be restructured to accommodate the imminent evolutions.

7th APPSNO Alumni Distinguished Dinner Lecture

Innovations and National Security
Peter Ho, Chairman, URA Board; Senior Advisor, Centre for Strategic Futures; Senior Fellow, Civil Service College, Singapore

In a world characterised by uncertainty and disruption there is a need to build innovative and resilient organisations capable of adapting to provide necessary solutions.

Distillation

1. Disruptive trends will continue at an accelerated pace.

2. The national security landscape is harder to control and predict as national security measures are no longer as effective and more resources are needed to identify and resolve threats.

3. Resilience against today's national security issues entails cognitive awareness, reflexivity and innovative solutions.

Distinguished Dinner Lecture

Defence Innovation
Christopher Kirchhoff, Partner, Defence Innovation Unit Experimental (DIUx), United States

The key factors in ensuring a security/defence organisation's strategic edge are a culture of continuous learning, helmed by proactive leaders, and partnering with the commercial sector (including start-ups) to harness technological innovation that could be potential game-changers.

Distillation:

1. In order to harness technological innovation to enhance security, there must be a culture of continuous learning, and partnerships between public and commercial sectors, including new start-ups. This will also require greater tolerance of risk and failure by government organisations.

2. Government organisations need more agile internal processes in order to keep pace with technological change, and draw more interest from the commercial sector to collaborate in developing security/defence applications. This is crucial as the commercial sector is outpacing the public sector in terms of R&D expenditure and developing technological expertise.

3. Policymakers from various areas (both security and non-security agencies) have to come together early to appreciate the potential positives and negatives of emergent technologies taking into consideration the intersectionality of different spheres such as the spheres of security, economics, and civil rights. This requires technical expertise, and hence, government organisations could draw upon technical expertise and recruit talent from the commercial sector.

Session 1: Innovation and Technology

The Challenge of the 21st Century—Embedding Safety and Security in a New World of Smart Cities

Simon Moores, Director of Research, Zentelligence (Research) Ltd, United Kingdom

Simon Moores

1. There has been exponential growth in computing power and data storage. As societies build even more complicated systems there is also an increase of potential failure points.

2. The complexity of today's technology hides the potential for negative externalities and second-order effects. For instance, a minor shift in search engine algorithms can wipe out the online presence of a small business.

3. The speed of urbanisation may mean that before building smart cities, there must be a priority to first build safe cities.

4. As the Internet of Things (IOT) grows, the attack surface for bad actors also expands. It is estimated that by 2030, 100 trillion sensors will comprise the IOT.

5. Smart cities may evolve organically as part of a technology-based societal change, but this is hindered by the fragmentation of information technologies where legacy systems need to be integrated with emerging systems.

6. As privacy and security concerns emerge out of the increasing complexity of smart devices, the importance of embedding trust in systems is necessary. Blockchain technology could provide this element of trust by distributing the storage and verification of information though a collaborative peer network.

Managing Multi-way Cyber Insecurity Dilemmas in Asia
John C Mallery, Research Scientist, Computer Science & Artificial Intelligence Library, Massachusetts Institute of Technology, United States

John C Mallery

1. There is accelerating instability in the international security system. Threat actors are now able to open up new channels of conflict. Adversaries increasingly target each other's C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) systems.

2. Strategic technological competition is now the norm. States are becoming locked into continued development of cyber capabilities. The state of world cyber forces is characterised by expanding capabilities. There are 29 states opting to build their own cyber weapons with another 49 procuring their capabilities from commercial sources.

3. The substantial amounts spent to procure ICT (4 billion USD) equipment highlight the need to address the potential points of vulnerability. Individuals remain oblivious to the increasing ease with which vulnerabilities can be exploited by malicious actors. Building systems that are secure by design will reduce vulnerabilities.

4. As confidence in military deterrence wanes, there is an increased risk for mistrust and escalation to lead to conflict. There are increasing

incidents of attacks just below the threshold of armed conflict. A "cyber insecurity dilemma" is currently unfolding, which can be resolved through cooperation between states. However, this is hindered by the lack of agreement over which values should be adhered to.

5. Initial steps have been taken to build cooperation between states, such as efforts by the United Nations Group of Governmental Experts (UN GGE) to develop norms to spare civilian infrastructure from cyber-attack.

6. It is important to have both cyber defence and cyber risk reduction strategies. Cyber deterrence could be a guiding principle for these strategies, which would include punishing and denying other states for wrongful behaviour. Cyber arms control could also be pursued, taking lessons from the experience with nuclear proliferation. The ultimate goal of any arms control regime is to make offense obsolete.

Singapore's Cybersecurity Strategy – Not Just Technology
Benjamin Ang, Senior Fellow and Coordinator, Cyber Programme, Centre of Excellence for National Security, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Benjamin Ang

1. Launched in October 2016, Singapore's national Cybersecurity Strategy is comprised of four pillars. The strategy reflects the unique national security approach of Singapore.

2. The first pillar is "Building a Resilient Infrastructure", which is comprised of 11 sectors including public utilities and the transport sector. Measures that comprise this pillar include the creation of National Cyber Incident Response Teams (NCIRT) and the establishment of a separate network for the civil service.

3. The second pillar is “Creating a Safer Cyberspace”, which calls for a collective strategy against cyber threats. Business should be reminded that security is a business imperative and not just a government responsibility.

4. The third pillar is “Developing a Vibrant Cybersecurity Ecosystem”, where a professional workforce trained for cybersecurity will be cultivated through educational and labour training programmes. There is interest in the Singapore Armed Forces to integrate “cyber conscripts” as part of mandatory National Service.

5. The final pillar calls for “Strengthening International Partnerships”. This includes the ongoing Singapore initiative for ASEAN Cyber Capacity Building. Another way partnerships are made and nurtured is through events such as the annual Singapore International Cyber Week.

6. In conclusion, it was highlighted that cybersecurity requires more than technology alone to succeed. It is important that technology is fused with appropriate processes and the nation’s human capital.

Syndicate Discussion

1. *Increasingly, more aspects of human lives can be considered “Critical Infrastructure”.* Democratic and electoral processes are now regarded as “critical infrastructures”. This is evident from recent allegations of Russian interference in the US elections in 2016.

2. *Smart phones should also be considered as “critical infrastructure” as they provide data that can significantly impact human lives*.

3. *Newer and more innovative ways of integrating data, especially in smart cities, should be developed*. Unified portals in cities such as New York and London provide examples of the possibilities of utilising open data for analytical purposes.

4. *The debate over privacy and government access to data will persist*. Legislative proposals such as the US Congressional vote to share or sell information obtained from individuals through Internet Service Providers (ISPs), and the United Kingdom’s Regulatory and Investigation Powers Act, allow governments to access metadata from ISPs. This raises concerns as individuals’ rights to privacy could potentially be violated. A sign of a healthy democracy is the advocacy and respect for data privacy.

5. *Trust-building and collaboration between white hat hackers and the government*. There can be more collaboration between the white hat community and the government. For instance, Tesla offers up to US$10,000 as a reward for uncovering vulnerabilities in its software. Hackathons such as the Hack-in-a-Box conference and bug bounty programmes organised by Microsoft enable trust-building between the community and stakeholders.

6. *Trajectory for smart cities*. The scale of technological development and the evolution of "electronic governments" are significant when determining the trajectory of smart cities. Countries aiming to be smart cities have to scale their development according to their comparative advantages, and specialise in a specific area.

7. *Implications of increased technology in smart cities*. The continued evolution of the Internet of Things (IoT) would lead to a society which is increasingly under surveillance. The availability of more resources and budget in smart cities compared to peripheral towns would lead to more technological developments in the former, and inevitably more policing as well.

8. *Establishing norms in cyberspace*. Many existing global norms are Europe-centric, and there is no international consensus on cyberspace practices. For example, the concept of "privacy" may be regarded differently in Asia as compared to Europe. Therefore, this would impact how governments seek to control content and/or behaviour online.

9. *The need for buy-in by CEOs and the boards of organisations to increase cybersecurity budgets*. Allocation of resources and budgetary constraints will always be an issue, and it is difficult to convince CEOs and board members why organisations need cybersecurity professionals. They are largely concerned about immediate profits, and as such, investing in cybersecurity may not be a priority. There is a need to increase their awareness of potential cyber threats, and urge them to invest in more robust cybersecurity measures.

10. *The importance of information sharing in the private and public sectors*. The term 'information sharing' is often confused with 'information offering'. The latter refers to the offering of information under certain frameworks, in agreement with two or more willing parties. Information sharing is usually voluntary and non-transactional. In the Singapore context, open dialogue and sharing is paramount to setting a norm of sharing knowledge.

11. *Categorising cyber threats to include attacks by non-state actors*. Cyber threats should be categorised so as to understand which deterrent strategies should be applied against which particular threat motivation. This will aid in recognising the correct resources and strategies to be applied in specific contexts. State actors usually have very different resources and objectives from non-state actors, and hence different deterrence thresholds.

12. *Whether a country can take a defensive position only (with regard to cybersecurity) and still remain secure*. Ideally, countries should possess both offensive and defensive capabilities to enhance cyber security. As adversaries subvert a country's dependencies, resilience would entail having more resources than the adversary. If a country is dependent on defence, then the defensive strategies need to change and develop fast enough to confuse the adversary. The best strategies are when offensive and defensive capabilities are merged.

13. *Most Internet of Things (IoT) devices do not have security embedded in them*. Critical infrastructures of cities are increasingly vulnerable as such more of such IoT devices are being integrated into city-wide technologies. Security depends to a large extent on the evolution of city-states. Some city managers have better contingencies than others to deal with IoT breaches, and can set up the necessary infrastructure to cope.

14. *There may not be enough jobs in the future*. Jobs are disappearing faster than they are being created. Furthermore, with increasing automation, real salaries are stagnant or have been decreasing since the 1990s. Economies around the world are not prepared for the rapid and inevitable use of artificial intelligence (AI).

Distillation

1. Further comparative analysis is needed to identify common issues faced by cities aiming for smart city status. This can help ensure a comprehensive whole-of-nation approach towards achieving the Smart Nation goal.

2. Policies are needed to increase awareness of decision-makers to cybersecurity threats facing the Smart Nation.

3. There is a need to carefully evaluate what services should be considered cyber information infrastructures in a Smart Nation, so that appropriates policies and measures can be taken to protect them.

4. The range of critical infrastructure vulnerable to cyber-attack has evolved to include non-physical assets such as electoral processes.

5. Emerging global norms should take into consideration the growth of cyber insecurity, the intensification of asymmetric conflicts, and the blurring lines between civilian and military targets, because existing norms that cover conventional warfare and state-level conflict may be inadequate at present.

Session 2: Resilience in the Post-Truth Era

The Weakest Link to Resilience: Establishing a Credible Reputation Defence in a Post-Truth Era

Ryan Lim, Founding Partner; Principal Consultant, QED Consulting Pte Ltd., Singapore

Ryan Lim

1. With the proliferation of social media and digital communication technologies, hoaxes and fake news are part and parcel of daily life today. An undiscerning public is the weakest link of resilience. There is thus a critical need to understand human behaviour to build resilience.

2. The private sector, while limited in terms of security and access to data, has the financial resources to focus on understanding consumers and markets. It also regularly deals with hoaxes and fake news and as such its experiences may be of great value to government agencies focused on building resilience to fake news.

3. The public has a short attention span and this limits its capacity to discern if information received is true before digesting it. Determining the validity of information is dependent on three simple factors: First, the degree of separation from the news. Friends and family play a critical role. Second, a large number of sources sharing the news lead to a greater perception of validity. Last, a semblance of credibility, from either the social media platform it is shared on (e.g. blue ticks), or a previously encountered source of information, leads to an assumption of validity.

4. Discerning the validity of information is sometimes difficult, even for professionals, largely due to the need for speed in response and the vast range of information being released constantly.

5. Commercial entities realise that building resilience against hoaxes and fake news targeted at them is essential for their commercial survival and employ three main strategies to counter these threats.

6. The first strategy is to establish a strong social media presence and build strong branded communities to directly disseminate information and quell hoaxes. This strategy allows commercial entities to reach out to their customer base directly through social media platforms and allows them to take a carefully curated position on issues.

7. The second strategy is one of digital advocacy, which involves building up a digital grassroots movement of sorts of trained volunteers through open dialogue and opening up a feedback loop that functions both ways. This method is highly effective in terms of tackling blind spots through reportage. Volunteers are guided and armed with information, rather than instructed, and are allowed to tackle hoaxes and disseminate information through their own networks, in their own way, making the message far more effective and credible. Digital advocacy is also very effective in terms of dealing with customer dissatisfaction and rumour mongering by defending the brand and tackling difficult customers on social media platforms in a way that commercial entities cannot.

8. The third strategy is to use diverse tools such as digital news velocity detection that allows commercial entities to identify which issues attract more attention and interest from consumers. Another tool that is used is digital psychometric analysis that allows analysts to work around the limits of sentiment analysis and surveys by looking at the digital footprints of consumers to draw stronger conclusions about consumer motivations and interests.

Russian Influence and Disinformation Operations in Europe
Jakub Janda, Head, Kremlin Watch Programme, Deputy Director for Public Policy, European values Think-Tank, Czech Republic

Jakub Janda

1. The Russian Federation uses seven major tools to influence domestic affairs in Europe. These seven tools synergize with one another and contribute to the greater cause without consciously working together.

   The first is the use of its influence in intelligence operations, not only in espionage but also through proxies, some of whom work in the offices of specific policy makers.

   The second tool is disinformation operations that create disinformation narratives through official channels, through proxies as well as allies. This enables the creating of echo chambers which allow the narrative to be repeated over and over again.

   The third tool is the use of political allies who are often politicians in targeted countries who subscribe to Russian foreign policy objectives, intentionally or otherwise. Some of these politicians have already been voted into office across Europe.

   The forth tool, most commonly observable in the Baltic region, is the strong presence of orchestrated NGOS. These NGOs are either Russian compatriot organisations, religious organisations tied to elements of the Orthodox Church or cultural organisations. They are often used for socio-political and cultural messaging.

The fifth tool is support for local extremists and radical groups. This support could be financial, material and resources based or even an invitation to Russia in a sign of symbolic support to strengthen their credibility amongst potential and existing followers.

The sixth tool is leveraging and targeting sections of disenfranchised ethnic minorities for espionage and spreading influence.

The seventh tool is economic operations with political goals to spread Russian influence in often seemingly innocuous ways.

2. The protection of democratically elected politicians and elections, the protection of democratic institutions like the media, and membership in EU and NATO, are three key factors that have to be protected in the fight against such a wide array of tools and strategies. The trust between citizens and these three factors is also sacrosanct and must be protected with utmost care.

3. Even countries in Central Europe or Western Europe show signs of having been subjected to disinformation campaigns that have focused on assigning blame for international issues on other countries like the United States. This takes attention away from Russia and indirectly promotes a non-threatening image of Russia.

4. The responses to Russian campaigns range from countries (like Greece and Slovakia) that deny the existence of such campaigns and do nothing about them, to countries that are beginning to feel the threat (like the Netherlands and Finland) and finally countries like the Baltic states who have always been aware and guarded for decades.

5. There are several reasons why there has been a lack of tangible political response in many countries towards this threat. First, there is a lack of credible data with little research being done on the impact of these information operations. Second, there is also distinct lack of advocacy and policy assessments at present, largely due to the fact that this is a new issue to many European states. Third, countries also do not want to be seen as censoring or conducting surveillance for domestic political reasons.

6. Kremlin Watch offers a list of 50 strategies that can be adopted to fight disinformation campaigns with 4 key response areas. This involves putting foreign interference and disinformation campaigns on the official security policy to ensure that institutions have to respond to them, as well as challenging the campaigns in the public domain.

7. Exposing the vehicles and tools of influence is also essential and needs to be specific and targeted.

8. There is also a critical need to build resilience against disinformation campaigns. However this has to be done in a non-aggressive fashion with an understanding that it takes years, often a generation, to have a big impact.

Integrating Resilience in Defence Planning against Information Warfare
Janis Berzins, Director, Centre for Security and Strategic Research, National Defense Academy of Latvia, Latvia.

Janis Berzins

1. Understanding information warfare and disinformation campaigns is to understand that it is not always about creating alternative realities through the spreading of lies. Instead it is also possible to tell a lot of lies, just by telling the truth in an alternative fashion.

2. There are several forms in which citizens 'exit' (i.e. disengage from) their states, namely political, economic, social, informational and cultural. This is often a reflection of a breakdown of the relationship between citizens and the state and the social contract that binds them.

3. It is important that issues like the election of Donald Trump and Brexit are not seen as solely due to external disinformation campaigns. That would be a gross over-estimation of Russia's or any external actor's capabilities. Rather, disinformation is most effective when people feel disenfranchised and convinced that the social contract has been broken for decades.

4. There are several main leanings of disinformation in the world right now, including the United States Alternative Right, the United States Alternative Left, The International Anti-Globalists, Muslim Defence and Russian Propaganda. The key denominator is these very diverse ideological disinformation campaigns is a focus on anti-globalism and a strong distrust of the western, democratic socio-political model. There is also a strong sense of disdain against neo-liberalism.

5. Berzins presented a case study of Russian disinformation operations in Latvia. He observed that the operation was not focused on getting the population to love Russia or President Putin, but instead used NGOs to Russian promote values and morals as being normal and inherent in Latvian culture and traditions.

6. Modern warfare has undergone a very critical change in the last few years, with the focus today being on the ability to influence the adversary's citizens. Rather than attempting to cause annihilation of the enemy state, there is increasing focus on trying to engineer its inner decay. In this way, war becomes a permanent state of being, rather than a limited engagement over a definitive period of time.

7. This modern warfare involves several key methods and objectives. One method is the stimulation and support for armed action by separatist groups with the objective of promoting chaos and territorial disintegration. It also involves highlighting and expanding the polarisation between the elites and society, resulting in a crisis of values.

8. Another key objective is stimulation of a socio-economic crisis and the incitement of mass panic creating loss of confidence in key government institutions, along with the defamation of important political leaders who are not aligned with the political interests and agenda of the aggressor state.

9. The focus is on using every available means to destabilize the political system and promote unlawful and subversive forces within the state as a distributed attack on the country's social cohesion, ideological core and political stability, much like a virus. Attempting to fight such a virus like attack is complicated. Democratic countries cannot adopt oppressive methods like the oppression of socio-political actors or the suppression of alternative media or information sources.

10. One strategy is to comprehensively monitor the information environment and resilience to information warfare within the country. Resilience must be operationalised by measurable criteria and monitored on a regular basis.

11. At a cognitive level, there must be a focused attempt at explaining the adversary's strategic goals and tools to the public. This requires being open and honest with citizens and getting them on board with being vigilant as well.

12. Doing this will require a national level strategic communications programmes targeted at winning hearts and minds of the citizens. It will also require programmes focused on enhancing critical thinking skills within the population and promoting high quality journalism. There is also a need to look at ways in which governments and society can interact directly without the media. This will also allow governments to get feedback directly from society.

Syndicate Discussion

1. *A hybrid response is needed to deal with online content management*. The automation of processes utilising algorithms allows for the tracking of keywords when entered online.

2. *A consumer journey funnel can be utilised to model individual trends online for the commercial world*. The consumer journey funnel is comprised of six points: (1) awareness generation; (2) awareness education, where consumers identify the touch points with the organisation to find out more information; (3) consideration, where consumers conduct a comparison with competitors against an organisation; (4) action point; (5) loyalty; and (6) advocacy. Social media audits can be conducted to check the robustness and adequacy of the existing digital messaging efforts, procedures and executions of organisations especially in times of crisis. Tonality analysis can be used to review and adjust the messaging disseminated online.

3. *Key points when building a branded community*. It is important to identify leaders within the community, and ascertain their suitability as ambassadors by analysing their psychographic characteristics. This ensures that their values are aligned with the organisations' goals. Utilising micro-influencers rather than over-relying on certain macro-influencers within the online community can maintain the credibility of these digital community leaders and prevent digital fatigue.

4. *Disinformation and propaganda campaigns in Russia*. The Kremlin regards diplomatic efforts by some Western countries as attempts to undermine Russia. To address this, Russia utilises Russian speakers residing in European Union countries and Russian state television broadcast channels, such as RT and Sputnik, to advance its interests. These media also serve to reinforce narratives that paint the Kremlin in positive light. When designing its propaganda materials, the Kremlin takes into account the social and cultural elements of the target, and tailors its messages accordingly. Ukraine, Syria and Germany are targets of the Kremlin's propaganda efforts.

5. *Disinformation has great power to influence public policy, and it is under-researched*. Although there is almost no public data available on how disinformation tactics are used to influence public policy, anecdotal evidence suggests otherwise. For example, Russia has been widely accused of using disinformation to achieve its foreign policy objectives.

6. *The role of the private sector on the issue of disinformation*. Technical policy responses are essential to identify and prevent disinformation from spreading. Commercial entities are usually unwilling to be involved in state politics; hence it is imperative for governments to engage them to discuss information, ideas, and policies. Ideally, governments and private companies should collaborate and share best practices in dealing with disinformation in a non-partisan manner. However, governments need to develop frameworks where collaboration is mutually beneficial to both public and private sectors.

7. *The media industry can help manage the spread of disinformation*. Governments should work closely with the media to establish protocols on how to manage disinformation. Governments need to discuss their policies openly with media to foster better engagement.

8. *The social contract between government and its citizens is being eroded globally*. Countering disinformation in Western countries is challenging as freedom of expression and information are essential societal values. Many people in Western countries do not trust their politicians and government. Fake news disseminated through social media has exacerbated the trend.

9. *Online platforms have a responsibility to mitigate negative comments*. The law is different for each state, and therefore it is difficult to determine who should be accountable or responsible for the repercussions stemming from negative comments on online platforms. However, states and online platforms should cooperate to mitigate negative comments when there is a need.

10. *Cyber-related techniques may be used to influence results of large-scale state elections*. A case in point is the 2016 US Presidential election, which involved hacking, publishing disinformation/fake news, and influencing the public digital domain (by using bots to influence online debates in forums). It has become a contentious issue in Europe, where French presidential candidate Marine Le Pen has been accused of using bots to bolster her online popularity. Meanwhile, German Chancellor Angela Merkel has cautioned that social bots may manipulate public opinion.

Distillation

1. There is an urgent need to build resilience against disinformation and fake news. Such a strategy must be non-invasive, non-aggressive, and will take time.

2. Building this resilience will require constant vigilance and monitoring of the information environment as well as the ability to operationalise the term resilience by measurable criteria.

3. Resilience building will also require a wide range of policies. This includes targeting the cognitive capacity of the polity by equipping them with the skills necessary to recognise hoaxes and fake news, as well as effective policies and effective strategic communications that communicate accurate information to the people and win both hearts and minds.

4. The private sector may be an effective resource from which states can learn how to build effective strategic communications strategies as well as how to build effective resilience against disinformation.

5. Further research is needed to understand how cyber-related techniques can be used to influence state decisions (e.g. elections) and how this can be circumvented or prevented.

Session 3: Innovation in Terrorism and Counter-Terrorism

Developments in Counter-Terrorism
Ali Soufan, Chairman and Chief Executive Officer, The Soufan Group, United States

Ali Soufan

1. Al-Qaeda (AQ) went through several mutations before and after 9/11. From 2003, AQ became a movement that started to attract affiliates all around the world. The founder of AQ Osama bin Laden was killed in 2011, but the "Arab Spring" that erupted at the same time provided AQ with a new opportunity to reinvent itself.

2. Three incubating factors of the global Jihadist movement can be identified: Sunni and Shia sectarianism; the "Arab Spring" and the war in Syria. The youngest generations are the victims of civil wars in which Jihadist groups like AQ and Islamic State (ISIS) are active. In Syria, 85% of the children are directly affected by the war, and one school out of three has been destroyed.

3. The threat landscape has changed, with the professionalisation of online Jihadist propaganda, and the increasingly dominant role of so-called "lone wolves" in the preparation and the execution of terror attacks.

4. These individuals increase the pressure on intelligence and law enforcement agencies as the gap between radicalisation and mobilisation is shortened.

Re-examining solutions to Countering Violent Extremism: building effective community-led interventions
Clarke Jones, Australian Intervention Support Hub (AISH)

Clarke Jones

1. To be effective, CVE programmes cannot be government-driven only. There is a crucial need to better understand the changing threat environment and improve society's early warning system, as cases of violent radicalisation may involve individuals that were not necessarily initially considered to be suspects. Therefore, working with families and young people at the community level is essential.

2. Intervention programmes need to be locally-driven and involve tailor-made religious and cultural responses. Different population environments make it impossible to apply a one-size-fits-all approach that does not take into account local particularities. Programmes must also present relevant cultural and religious answers to young people from different backgrounds.

3. Expressions such as "radicalisation", "de-radicalisation" and "countering violent extremism" can be perceived as offensive by some individuals and communities. CVE practitioners should be flexible and figure out different engagement approaches. Another mistake is for authorities to favour top-down and risk-based approaches that label individuals as threats, as this alienates the communities.

Risk Assessment for Violent Political Extremism: National Security Applications

Elaine Pressman, Netherlands Institute of Forensic Psychiatry and Psychology

Elaine Pressman

1. The phenomenon of returning foreign fighters makes it crucial to identify individuals that are likely to pose a higher threat within that particular group of people.

2. The fundamental objective of the formal risk assessment system is to assess the likelihood that an individual will act in a harmful way. It also evaluates the type and severity of harm that the individual may cause and aims at determining what action to be taken to minimize the risk and threat.

3. Informal risk assessment approaches that are only based on subjective elements such as the intuition and experience of analysts are limited. The structured professional judgment (SPJ) is the best approach. This methodology requires analysts to assess the information included in a structured protocol and to derive meaning from the information. The value of the SPJ is to combine scientific methods of data collection and processing with professional judgment.

Syndicate Discussion

1. *The community-based approach is advocated as the middle-ground to build support and buy-in from the community*. The government might not be in the best position to oversee efforts to reach out to schools or religious institutions that are considered ‘sacred spaces’ within the community. Such efforts should be done by community leaders

and supported by the government. In order to sustain community buy-in as well as reduce suspicion within the community, a step-by-step intervention and a long term engagement strategy is needed to understand the dynamics of the community.

2. *Effectiveness of engagement efforts in Muslim communities*. Muslim families and communities are increasingly weary of engagement efforts by the authorities. There should be respect for the communities' privacy, and there should not be any assumptions that the community need engagement. Long-lasting trust should be built to prevent the communities from feeling they are being monitored unfairly.

3. *The Islamic State of Iraq and Syria (ISIS) as a 'digital disrupter'*. ISIS mass-markets its ideologies as highly personal and models itself as an 'Uber' or digital disrupter of the global jihadist movement. Its global movement involves local ownership and it operates much like the Starbucks franchising model by using local affiliates under the main ISIS umbrella. Al-Qaeda could, in time, frame its messages to be attractive and relevant to millennials.

4. *"Kill the message, rather than the messenger"*. Counter-terrorism strategies should aim at strategically framing counter-narratives to prevent echo chambers and the spread of terrorist ideologies.

5. *Use the right messenger*. The use of religious leaders for interventions, while necessary and important, may not be applicable in all instances. Finding an individual who is respected by the target audience (e.g. those with 'street cred' who resonate with teenagers) is extremely important for counter-messaging efforts.

6. *Al-Qaeda is reinventing itself and should be monitored closely*. Al-Qaeda's resilience should not be underestimated. ISIS' and Al-Qaeda's ideologies and narratives overlap, and the former could re-emerge.

7. *Returning foreign fighters*. Many countries face issues related to returning foreign fighters. For example, returning fighters from China are from the Uighur community. However, many of them settle in Turkey instead, where Turkish laws allow descendants of Turkish origins to reside in Turkish territory. This may pose future problems of radicalisation for Turkey, as more Uighur fighters settle there.

8. *Spill-over effects on Asia from the Middle East*. While the threat of returning foreign fighters remains, local terrorist groups in Asian countries are just as dangerous. Terrorist networks in the Middle East are rapidly

spreading out to Asia. A consequence of geopolitical problems in the Middle East is that entire generations in "at-risk communities" are growing up without education and a place in the formal world economy. This may fuel radicalisation further.

9. *Balancing risk-based approaches with support interventions*. Risk-based approaches and support interventions are independent of each other. Risk-based approaches should not be used to model intervention. While risk assessment should be used to protect the safety and security of society as a whole, it is not appropriate for use in schools.

10. *Increasing number of lone wolf attacks has made risk assessment more challenging*. The lone wolf phenomenon is problematic when it comes to individual risk assessment because there is usually little or no information available about the attacker. However, lone wolves are not really alone – they are virtually attached. Therefore, the trajectory of risk is observable to some extent in their cyber or online behaviour.

11. *Using Artificial Intelligence (AI) to support terrorism risk analysts*. The Pacific Northwest labs in the US are working with the FBI to use Big Data to support terrorism risk analysts. While this initiative is commendable, it may not be useful when attempting to find individual suspects. AI is not sophisticated enough yet to make analyses yet; risk assessments need more individualised approaches.

12. *If multiculturalism is not supported, then the number of violent acts could increase*. In the near future, extreme violent acts may not necessarily be religiously-motivated but motivated by social cleavages or fault lines. The focus on developing multiculturalism within societies is diminishing in many countries. Policy shifts are required to combat Islamophobia. Integration as well as reintegration efforts need to be in line with multiculturalism efforts.

Distillation

1. The threat landscape has changed with the professionalisation of online Jihadist propaganda and the increasingly dominant role of so-called "lone wolves" in the preparation and the execution of terror attacks. These individuals increase the pressure on intelligence and law enforcement agencies as the gap between radicalisation and mobilisation is shortened.

2. Expressions such as “radicalisation”, “de-radicalisation” and “countering violent extremism” can be perceived as offensive by some individuals and communities. CVE practitioners should be flexible and figure out different engagement approaches. Another flaw is for authorities to favour top-down and risk-based approaches that consider individuals as threats.

3. Structured professional judgment (SPJ) is arguably the best approach for risk assessment in radicalisation. Analysts are tasked with assessing a structured protocol containing a large volume of data and interpreting the information contain therein. The value of the SPJ is the ability to combine scientific methods of data collection with professional judgment.

4. European governments need to evaluate if there has been excessive monitoring of the minority Muslim communities, and if the strategies employed thus far have been effective. They need to develop diverse community-based approaches to deal with the threat of radicalisation. Individual treatments that allow CVE practitioners to tailor their intervention to particular cases constitute an important best practice.

5. The international community should not underestimate AQ, as it is growing more powerful.

6. The 2016 VERA 2R protocol was specifically developed for risk assessment of radicalisation leading to violent extremism. Based on empirical information and a comprehensive range of indicators, it is used by the police, intelligence and military communities in various countries. The key benefit of such a model is to provide a reliable and evidence-based approach to risk assessment.

Session 4: Innovation in Strategic Communication

Multi-Platform (UAV, UGV, and Mobile User) Information and Communications Systems for Disaster Risk Reduction
Gregory Tangonan, Professor, Founding Director, Ateneo Innovation Center, School of Engineering, Ateneo de Manila University

Gregory Tangonan

1. Technology can aid situational awareness during disasters and emergencies. V-Hub technology was used to provide communications to support disaster recovery in the Philippines. Facial recognition technology was used to identify individuals during a disaster, and unmanned aerial vehicles (UAVs) were used to determine the location of survivors. V-Hub technology ensures communication is not disrupted even if conventional mobile networks fail.

2. Most countries, even developed nations like Japan, are taken by surprise when a natural disaster strikes. It is therefore crucial for countries to prepare for such emergencies by conducting evacuation procedure drills. Stakeholders should seek to understand the local community's social connectivity prior to an emergency in order to formulate a more effective disaster response.

3. International cooperation and information sharing is important for disaster management. Currently the Philippines is collaborating with organisations in Japan and Southeast Asia to make V-Hub technology the new Asian standard for disaster communications.

4. The Ateneo Innovation Center plans to use technology to provide mobility devices to the disabled. As companies seek to move into car-sharing, mobility devices such as wheelchairs and walkers can be repurposed as dual-use devices (communications and mobility).

The Role of Media Literacy in Combating Fake News
Lock Wai Han, Chairman, Media Literacy Council; Chief Executive Officer, OKH Global Ltd.

Lock Wai Han

1. The impersonation of official websites and social media accounts, as well as digital alteration of pictures and videos, has made it increasingly challenging for individuals to separate fact from fiction in the online space.

2. Altruism tends to be the motivation behind sharing of online content, but if the information is incorrect, the spread of such misinformation negatively impacts organisations and individuals.

3. In tackling misinformation online, stakeholders need to grapple with the question of responsibility, deciding which party should be responsible for: (a) verifying information; (b) reporting an incident (social media platform, organisation, affected person, or relevant authority); (c) investigating the incident and prosecuting the perpetrator; (d) eradicating the source of misinformation; and (e) restoring normalcy.

4. The Media Literacy Council (MLC)'s role is mainly to teach individuals how to be more discerning online and protect themselves against cyber threats (e.g., cyber bullying). MLC advocates four core values as the basis of online conduct: empathy, respect, responsibility and integrity. It also conducts research to generate new ideas and provides thought-leadership on digital-related issues. The MLC runs an annual Better Internet Campaign, and cooperates with both public and private agencies to conduct events that promote media literacy.

5. While public education and instilling corporate social responsibility are important, the responsibility for critically evaluating online sources ultimately rests with the individual. Therefore, future campaigns will aim to bolster digital maturity in individuals.

Challenges in the Social Media and Communications Landscape
Alvin Tan, Head of Public Policy, South East Asia, Facebook

Alvin Tan

1. As Facebook's user base expands globally, the social media company has established Community Standards to determine what users are allowed to post on its platform, forbidding content that extols hate speech, violence, spam, pornography, human trafficking, and identity theft. Content that violates Facebook's Community Standards will be removed if they are reported by other users or if flagged by the company's machine learning capability.

2. While Facebook has strict policies with regard to abusive content, it does allow for diversity of discourse among users. For instance, posts that challenge ideas, institutions, and practices and incorporate humour and satire are permitted. In order to promote responsible posting, Facebook encourages the use of 'authentic identity' among its users.

3. Facebook is working to address takedown requests in a more accurate and expeditious manner. Its review team works around the clock, and covers more than 40 different countries.

4. Facebook also considers counter-speech, a form of speech which challenges the speaker, to be an effective strategy against hate speech and violent extremism online. Some examples of counter-speech include: #IllRidewithYou (Martin Place attack in Sydney, December 2014),

#KamiTidakTakut (Jakarta attack, 2016), #JeSuisCharlie (Paris attacks, November 2015), and One Million Voices against FARC (Colombia, 2008). Counter-speech should be constructive and address the different nuances of extremism, for example differentiating between political Islam and violent forms of fundamentalism.

5. In addressing the challenges of hate speech and online radicalisation, Facebook seeks cooperation with a wide spectrum of experts to inform policies, and to engage credible voices from different age groups and religious backgrounds to counter violent extremism online.

Syndicate Discussion

1. *Hacking unmanned aerial vehicles (UAVs)*. The technology used in unmanned aerial vehicles could potentially be hacked. This would have grave implications as attackers would be in possession of high-resolution pictures of potential targets. They may also be able to switch on sensors on the UAVs meant for collecting additional data, and use the data for nefarious purposes.

2. *Challenges of identifying and defining fake news*. A key challenge is deciding how to define fake news in light of different cultures and norms. Fact-checking websites and tools can be disputed and accused of being biased or partisan. For instance, supporters of President Trump accused Snopes.com, an independent third-party fact checker, of advocating a partisan liberal agenda.

3. *Public education efforts in media literacy skills are important in combatting fake news.* Enhancing media literacy skills and building resilience in young people through public education efforts is important in combatting fake news. MLC is looking into producing handbooks for teaching cyber and media literacy skills to students e.g. how to differentiate between fake and real news.

4. *Generation gap and the use of technology*. Technology will evolve with each generation, and parents today find it difficult to teach children how to behave appropriately online. The Media Literacy Council has stepped in to bridge this gap by providing media literacy programmes aimed at school-going children. Programmes to teach senior citizens how to use the Internet more effectively have also been developed.

4. *Persistent legal challenges for social media companies*. Social media companies are bound by local laws in the countries where they operate,

and the cultural and/or local norms. Facebook carries out geo-blocking of content (blocking content in a specific country) where required.

6. *Echo chambers on social media platforms*. Social media platforms have algorithms that allow users to create echo chambers for themselves, where people with similar opinions form groups and discuss issues with little or no regard for alternative views. Narrow (or mistaken) interpretations of events may become accepted as 'fact' as group members reinforce each other's worldview.

7. *Responsibility for dealing with fake news*. There needs to be a whole-of-society approach to limit the spread of fake news. Singapore is fortunate that public trust in the government is strong, but this is not the case in many other countries.

Distillation

1. Further research is needed to find out how to help individuals critically evaluate online materials. This may include be more in-depth studies into echo chambers on social media platforms, particularly how they influence behaviour. It may also include comparative studies on the types of media literacy skills taught in various countries.

2. In order to combat fake news, a whole of society approach is needed, incorporating social media platforms, educators, legislators, fact checkers, citizens, and governments.

Session 5: Case Studies

Climate Change, Disaster Risk and Scientific Tools: Philippines Case Study

Antonio Yulo Loyzaga, Chairperson, International Advisory Board, Manila Observatory

Antonio Yulo Loyzaga

1. Disasters occur when climate and geological hazards overwhelm coping and adaptive capacity to govern risk. Understanding the nature, scale and dynamics of each element, and how these intersect to impact critical life support systems such as water, food and energy are at the core of risk reduction and maintaining national security in the Philippines.

2. Climate change presents two types of changes: shifts in normal levels of temperature, precipitation and sea levels; as well as increases in the frequency and intensity of natural disasters such as typhoons, floods and droughts. The Philippines is pressed between tectonic plates, increasing the risk of earthquakes and tsunamis. Geologists warn that Manila could be struck by a major earthquake soon, which would severely damage infrastructure.

3. Lessons learned from recent events include the need for Humanitarian Assistance and Disaster Relief (HADR) efforts to prepare for both rapid and slow-onset disasters, such as prolonged rainfall causing landslides.

4. Advanced scientific tools are crucial for risk identification and situational awareness to communicate risk among the public. In collaboration with NASA, the Philippines government is conducting research on tropical climatology and particularly the way aerosols affect the way rain is formed. Climate downscaling processes forecast possible scenarios and the potential effects of climate change. Light detection and radar (LIDAR) mapping is conducted to expose communities that are at risk of flooding and other environmental stresses in order to establish pre-crisis response plans. Results are particularly relevant to ensuring food and water security in disaster prone regions and municipalities.

5. Disruption and displacement during disasters also provide opportunities for insurgent groups to take advantage of uncertainty and frustration among local people, which has led to the establishment of alternative power structures and the instigation of violence toward authorities.

6. Research into mapping social vulnerability among Manila's informal settlements has been conducted for the past 20 years with regard to a possible earthquake and the various levels of need for different communities in the event of a major disaster. On a community level, the government is beginning to chart networks of trust and social capital to understand where influence derives and the differing levels of confidence residents have in state social service providers. One key finding has been that are very low levels of trust toward government officials and very high levels for family and friends. Emergency communications should be designed with these dynamics in mind.

7. A new tool that looks at HADR from a military-civilian perspective is being trialled in various ASEAN countries. It aims to find ways of facilitating the continuance of military humanitarian assistance among communities hit with significant natural disasters and enhance resilience and ongoing regional stability.

Hackers Lead the Way

Jeff Moss, Founder and CEO of DefCon Communications and the Black Hat Briefings

Jeff Moss

1. Hacking is an agnostic skill set, essentially neutral in its moral implications. A good hacker has high levels of inherent curiosity and understands the pursuit as a contact sport, requiring constant practice and hands-on experimentation. The term 'hacker' originally referred to the innovative pioneers of Silicon Valley, but when criminals moved online, the media used it to describe the perpetrators of internet crime.

2. The main actors in information security are nation states, which are predominantly motivated by keeping and obtaining secrets; money-focused organised crime syndicates; protesters or 'hacktivists' who demand attention for their respective cause; and hackers or researchers, who seek a deeper understanding of how systems work and how they can be influenced.

3. People generally fear what they do not understand and seek to control what they fear. Reductionist media misrepresentations of complex technical processes have vilified hackers, often leading to suboptimal policies and counterintuitive outcomes.

4. Governments should learn how to embrace and foster the talents of hackers. In the US there are federal minimum sentences for computer crimes and penalties have become more and more severe in the past 10-20 years. At present, hacking a computer is regarded as a more serious offence than drunkenly running someone down with a car and killing them. The unintended consequence is the accidental creation of criminals through counterproductive laws and policies. Incentives and

alternative outlets for positive contributions are much more effective ways of engaging young hackers.

5. Governments can take constructive steps toward engaging young hackers in different ways. One is through national cyber defence competitions, which focuses their energy toward defence through gamification and healthy rivalries. High school competitions provide off ramps for teenagers to focus their hacking skills on positive goals and similar initiatives are beginning to take place among even younger participants.

6. 'Bug Bounties' are an effective low-cost approach used by corporations and some governments to commend and reward individuals for exposing a cybersecurity vulnerability. The accolades are designed to incentivise young hackers to use their skills in constructive ways.

7. Manufacturers are not naturally forthcoming about faults and vulnerabilities in their products, so it is difficult for consumers to make informed choices. By exposing such vulnerabilities, hackers actually provide a public good that other actors are either unable or unwilling to offer.

National Security Implications of the Fourth Industrial Revolution
Linton Wells, President and Chief Executive Officer, Global Resilience Strategies

Linton Wells

1. The Davos World Economic Forum has identified four industrial revolutions. The first began in the 1780s when steam and water power drove machinery such as trains and mechanical looms. In the 1870s, electricity facilitated mass production and the division of labour. The

third came about in the late 1960s, with semi-conductors, personal computers, the beginnings of the internet, and robotics. Last year, a fourth revolution was identified, in which the fusion of technology such as robotics, information and Nano technology is blurring the lines between the physical, digital and biological spheres.

2. The key distinctions between the third and fourth revolutions are the velocity of change, the scope of change and the system-wide impact. Changes will be hugely disruptive, potentially providing important collective benefits to society but also negative individual consequences. Jobs will be lost. The pace of social change will increase. Responses need to be public and private; whole of government; transnational; and integrated. Linear projections are no longer relevant.

3. The new model will require redefined information sharing rules, whereby governments and militaries are more open to cooperation with civil society and the distribution of information. There will be major policy, legal, ethical and privacy issues which current decision-making processes are not suited to address. Furthermore, increasingly complex data will need to be visualised in more sophisticated ways, including the use of augmented and virtual reality.

4. The fourth industrial revolution is changing the way warfare is conducted. Cheap technology will pose challenges. Additive manufacturing allows actors with limited resources to 3D-print drones and explosive foreign penetrators (EFPs); nanotechnology is proliferating and automated intelligence is converging to allow for cheap, widely available autonomous weapons. The true centre of gravity of future conflict will not be tanks, troops, artillery and ships, but the minds, mobile devices, living rooms and populations of highly connected and engaged nations.

5. Labour markets will face significant disruption as automation replaces a range of occupations, notably in the service sectors. Technological developments will exacerbate inequality both within and among nations. The ‘youth bulge’ regions of South Asia and Sub-Saharan Africa will be affected in particular, with a lack of entry-level jobs potentially leading to increased migration, marginalisation, radicalisation and political violence.

6. The most profound change will affect us as people; evolutions are changing not only what we do but who we are. Biotechnology, artificial intelligence, and privacy issues are redefining what it means to be human. Extensions to current thresholds of life span, health, and cognition will require redefinitions of ethical boundaries.

7. Humans should not accept change passively but try to shape the future and work towards a comprehensive understanding of how technology is affecting lives. Outside-the-box thinking is irrelevant as the box no longer exists; humans must innovate, improve, repeat, and start again.

Syndicate Discussion

1. *A whole-of-society approach in crisis management and disaster relief is needed*. The private sector contributes significantly towards emergency preparedness and resilience efforts in the Philippines. For instance, 80 corporations including Coca Cola and Shell are grouped in disaster and emergency clusters (e.g., energy and power), which are activated pre- and post-disaster, complementing government and non-governmental organisation (NGO) efforts by plugging gaps in disaster preparedness and recovery efforts.

2. *Livelihood and geographical challenges abound for relocated populations*. While the relocation of vulnerable populations in coastal areas to secondary cities might save lives, the rebuilding of their lives in such cities is a challenge. The livelihoods and lifestyles of populations may be drastically affected. For instance, fishermen may see a reduction in the number of jobs they can undertake due to the geographical constraints in secondary cities inland.

3. *Fostering closer engagement with the public and hacking communities*. Bringing hacking closer to the community through initiatives such as Hack-for-Kids promotes 'hacking for good', and provides opportunities to spot and groom potential young talented individuals to consider a career in cybersecurity.

4. *The importance of networking in the technology industry*. Connections and networks made within the technological field are increasingly valuable. The rapid speed of technological change in the field has encouraged individuals to be specialists in selected areas of focus, rather than generalists. Therefore, there is a need to maintain connections with different individuals specialising in different aspects of the field in order to stay informed of the latest developments.

5. *Issues of accountability with regard to autonomous weapons systems*. Autonomous weapons are programmed to follow set rules, but it is unclear if the systems programmer or the commander of the military unit should take responsibility if an autonomous weapons system fails to carry out its mission.

6. *Increasing productivity levels is a challenge*. Singapore should develop its innovation culture further. It is already doing well to promote tech start-ups. The government may want to consider reviewing its bankruptcy laws to encourage entrepreneurs to innovate.

7. *Innovation and entrepreneurship have to respond to public sentiment on technological change*. If majority of the population are resistant to respond to technological changes, then innovation will not be profitable and inequality will deepen.

8. *The notion of 'ethical hackers' is fairly new*. Corporations have responsibility in ensuring that their staff members who are tasked with hacking are managed well and informed of risks involved. Cooperation between the public and private sectors is also crucial to identify potential security risks.

Distillation

1. Investment in environmental science research and innovative responses to disaster management are critical in the emerging era of increasingly frequent and severe weather events brought about by climate change.

2. Governments need to embrace the inherent curiosity and technical skill of young hackers who are often at risk of falling into criminal behaviour because of sanctions derived from counterproductive policies and disproportionately harsh legislation.

3. Studies should be conducted on policies for recognising hacking as a positive skillset, and how it can be harnessed for the benefit of society.

4. Global technological advancement, rapidly increasing complexity, and the fusing of biological and digital phenomena have such disruptive potential that entire societies may need to be restructured to accommodate the imminent evolutions.

7th APPSNO Alumni Distinguished Dinner Lecture

Innovations and National Security
Peter Ho, Chairman, URA Board; Senior Advisor, Centre for Strategic Futures; Senior Fellow, Civil Service College, Singapore

Peter Ho

1. Disruptive trends and accelerating change should continue to be expected in our complex and volatile world.

2. Globalisation and new technologies around cybersecurity and additive manufacturing contribute to the disruptions and capacities seen in the security landscape. Weapons are now more accessible, threats are harder to trace, and artificial intelligence may pose an existential risk.

3. The security landscape is now a war of attrition that is both innovative and asymmetric, with more resources needed to identify and resolve disruptive issues.

4. Cognitive biases create hesitation, crises and military failures. Hindsight is crucial in spotting trends and shaping factors that have a positive effect on the future. Horizon-scanning is informed by lenses that highlight challenges and opportunities. For example, the lens of urbanisation reveals how pressures placed on infrastructure and quality of life contribute to national security issues including pollution, poverty, crime and terrorism.

5. To cope with shock, a resilient organisation is needed. National security issues should be addressed through innovations that include but are not limited to technology. Examples include community processes, crowdsourcing for ideas and risk assessment systems.

Discussion

1. There is difficulty in calculating degrees of risk, security and corollary measures needed. Only when there is agreement among national security agents can resources then be allocated.

2. The pace of change is increasing quickly, driven by forces of technology, urbanisation and human impact on the environment.

3. Sustainable development goals require large resources. The difficulty of accruing sufficient economic resources on an international level is complicated by regional and national interests that limit the bandwidth of nation-states.

Distillation

1. Disruptive trends will continue and change will continue at an accelerated pace.

2. The national security landscape is harder to control and predict as national security measures are no longer as effective and more resources are needed to identify and resolve threats.

3. Resilience against today's national security issues entails cognitive awareness, reflexivity and innovative solutions.

Distinguished Dinner Lecture

Defence Innovation
Christopher Kirchhoff, Partner, Defence Innovation Unit Experimental (DIUx), United States

Christopher Kirchhoff

1. Innovation in organisations is enabled by a culture of continuous learning that is driven by good leaders who lead by example. Learning processes should be immersive, deliver new knowledge and experience, and include engagements with the commercial sector.

2. The locus of technological innovation is shifting to the commercial sector. The commercial sector's R&D expenditure - a significant portion is concentrated in start-ups - is surpassing federal R&D expenditure. New commercial technologies incubating in Silicon Valley now include hardware with promising defence applications.

3. The US Department of Defence (DOD) had to shift its lines of vision to maintain its technological edge by diversifying its business partnerships beyond the traditional few major defence companies to include new start-ups. The DIUx office was founded in 2015 to facilitate partnerships with start-ups, and to pilot and adopt emergent commercial technologies for defence applications.

4. The DIUx is organised into six practices: (a) Networking and Security; (b) Systems and Analytics; (c) Life Sciences; (d) Space; (e) Artificial Intelligence; and (f) Autonomy. Each practice has its own technical and business experts. As part of the DOD's innovation ecosystem, the DIUx specialises in harnessing late-stage commercial technologies which are developed by start-ups.

5. To access fast-paced technological innovation in the commercial sector, the DIUx could not rely on the Federal Acquisition Regulation (FAR) – an acquisition vehicle historically used to procure technology – given its time-consuming process to secure a contract. The DIUx instead chose to use Other Transaction Authority (OTA), which is a more agile acquisition vehicle, to compete with the consumer market in drawing the commercial sector's interest.

6. To identify problems and the commercial technologies that could potentially solve them, the DIUx first worked with military/defence agencies and including frontline officers (war fighters) to appreciate the problems. Relevant expertise was brought in to help navigate the commercial sector in the areas of: (a) technical due-diligence to assess the viability of the companies' products; and (b) business due-diligence to assess the financial strength and business models of start-ups. Finally, prototypes developed by the companies were piloted by military agencies.

7. To effectively reach out to start-ups across the country, the DIUx publishes every solicitation for commercial technologies on its website. Hence, proposals and bids for DIUx contracts have come in from 36 US states. DIUx now leads 24 projects with a total worth of 47 million USD in R&D funding. Notable projects include: (a) quadcopters that could be used by Special Forces to scan for threats in buildings, developed by Shield AI; (b) bone-conducting microphones that could be used by soldiers in combat zones, developed by Sonitus; and (c) fully autonomous sailboats that could support coastal surveillance, developed by Saildrone.

Discussion

1. The development of Artificial Intelligence (AI) and lethal autonomous systems such as drones is expected to be key factor of strategic stability in the future, comparable to nuclear weapons which can be both stabilising and destabilising. Present concerns over the use of AI in the military context are: (a) its predisposition to behave in completely unexpected ways; and (b) that the commercial sector would be way ahead of military/defence agencies in developing risk mitigation programmes for A.I systems. Hence, the adoption of AI for kinetic applications in the military must be pursued with caution.

2. While the timeframe between product conceptualisation and budget approval could be compressed, the timeframe between product development and launch entails a different set of challenges. For example, prototyping would involve the challenging process of closely integrating new technologies with existing operational systems. This process would require pairing start-ups with traditional defence contractors.

3. The DIUx, as a small office, is focused on the needs of the DOD. Nonetheless, it tries to cultivate a positive effect in the commercial market in two ways: (a) helping start-ups to grow - through a more agile acquisition vehicle - by pioneering new technologies with the DOD; and (b) helping start-ups to attain funding as venture capitalists are less comfortable in investing in defence projects given more funding required and higher risks perceived. DIUx also hopes to grow the interest of the commercial sector – entrepreneurs and investors - in the defence market.

4. The pursuit of innovation inevitably entails greater tolerance of risks and failure by the government. To only bank on “winning” companies would be too conservative.

5. Public-Private partnerships are important in the pursuit of innovation as the commercial sector possesses a wide range of expertise that governments lack. Governments could also attract talent from the commercial sector but this would require human resource policies that ensure attractive remuneration and job opportunities in the civil service.

6. Unlike in the past where advanced technology was the preserve of the military, many technologies of today are by nature dual-use and widely available in the global market.

   There are risks in developing dual-use technologies with the commercial sector. The democratisation of technology, driven by lower costs of technology adoption, could potentially enhance the capabilities of hostile non-state actors. This trend would increasingly have a profound effect in shaping the security environment especially in the current era where non-state terrorism is a major concern. For example, the availability of home-based kits to backyard scientists and hobbyists could enable genetic modifications on organisms. This could create new medical breakthroughs but could also create bio-threats.

7. The acquisition of US start-ups by other countries and the involvement of non-US researchers in the development of dual-use technologies have been highlighted in the US media as challenges to the national security and military superiority of the US

8. In the domain of national security, policymakers need technical expertise to address important issues that resulted from technological changes. Policymakers without technical backgrounds could partner with practitioners who may not be in the government but have experience in engineering (science and technology) and working in the commercial sector. These practitioners are expected to have an increasingly important role in policymaking and risk management.

9. Policymakers need to appreciate the potential upsides and downsides of emergent technologies, including security, economic and other implications that could overlap. There are no straightforward answers with respect to the regulation and risk management of these technologies. Hence, policymakers from these various areas (agencies) have to come together early to carry out horizon scanning and analysis of these technologies and its implications. Existing coordination frameworks in the government may have to be reviewed to foster better inter-agency collaboration and sharing of new technological capabilities.

10. Several lessons could be learned from the management of the Ebola outbreak: (a) there are serious risks as the operational capabilities to combat pandemics reside in small non-profit medical organisations and not large organisations such as World Health Organisation (WHO); (b) more pandemics could be expected in the future as growing urbanisation and global connectivity create conditions that facilitate the mutation and spread of diseases; (c) diseases that are asymptomatic or transmissible by air such as the influenza virus could pose greater risks of pandemic than the Ebola; and (d) early intervention is key in stopping pandemics given the speed of its spread.

Distillation

1. In order to harness technological innovation to enhance security, there must be a culture of continuous learning, and partnerships between public and commercial sectors, including new start-ups. This will also require greater tolerance of risk and failure by government organisations.

2. Government organisations need more agile internal processes in order to keep pace with technological changes, and draw more interest from the commercial sector to collaborate in developing security/defence applications. This is crucial as the commercial sector is outpacing the public sector in terms of R&D expenditure and developing technological expertise.

3. Policymakers from various areas (security and non-security agencies) have to come together early to appreciate the potential upsides and downsides of emergent technologies, including security, economic and other implications that could overlap. This requires technical expertise and hence, government organisations could draw upon technical expertise and recruit talent from the commercial sector.

Country Presentations

Singapore, Australia, Bahrain, Bangladesh, Brunei, Spain

1. A common national security threat identified by the countries mentioned-above was ISIS-inspired terrorism in the form of lone wolf attacks or large-scale attacks.

2. In terms of country-specific threats, drug trafficking was a major cause of concern for Singapore and Spain. For Bahrain, sectarian tensions/ violence spilling over from neighbouring countries was regarded as a major threat. Brunei viewed cyber threats as a growing concern. Bangladesh identified religiously-motivated violence as problematic.

3. In terms of solutions, Australia recommended better intelligence gathering from open as well as closed sources. Singapore discussed the SG Secure movement that aims to ensure citizens are prepared and can respond appropriately to national security threats. Brunei also alluded to strengthening community resilience.

4. All countries acknowledged the need for better international cooperation and collaboration to combat contemporary national security challenges.

Cambodia, China, India, Indonesia, Japan, Republic of Korea, Laos PDR, Malaysia, Myanmar, New Zealand

5. Two common threats to national security can be drawn from this set of country presentations. First, countries cited cybercrime as a present issue of concern. This included unauthorised hacking into government databases and cyber-attacks on government infrastructure.

6. Second, terrorism and ideological radicalisation were also identified as major threats to the countries mentioned above. This included potential terrorist attacks on strategic spots within the countries, and the problems brought about by returning foreign fighters.

7. Many countries called for greater cooperation to combat cybercrime and terrorism at the regional and national levels. Countries cited the need for increased capacity building across multilateral platforms via ASEAN or the European Union, and learning from the experiences of other countries in fighting these threats. This included sharing counter narrative experiences in fighting radicalisation.

8. For less developed countries such as Cambodia and Myanmar, there is a significant need to create legislation specifically for cybercrimes and terrorism, and reduce dependence on the local penal code for these acts.

9. While many highlighted cybercrime and terrorism as main national security concerns, some countries specified other issues as sources of concern. For example, New Zealand and the Philippines are most concerned with the impact from natural disasters and calamities, China and South Korea have had territorial disputes or diplomatic tensions. However, issues of drug and human trafficking are feared to be linked to terrorist groups, and may point to larger syndicate networks and coordination.

Norway, Pakistan, Philippines, Sri Lanka, Switzerland, Thailand, United Arab Emirates, United States, Vietnam

10. Common threats among the countries mentioned-above included: lone wolf attacks, organised large-scale attacks by terrorist groups like ISIS, and crisis management after an attack.

11. The representative from Pakistan spoke of the negative image of his country because of terrorism. The Philippines also faces serious threats from Islamists, but the government is wary of the threats posed by the Communists.

12. Norway identified the border with Russia as most vulnerable, and the UAE cited the sectarian divide within the Middle East as a significant issue for them in terms of domestic security.

13. Most countries included collaboration with regional countries and international organisations and blocs as the most viable solution to support counter-terrorism efforts. For instance, ASEAN countries (Philippines, Thailand, and Vietnam) mentioned the need to provide security for the whole ASEAN region, just as the European countries spoke of the importance of the European Union. Similarly, the representative from Sri Lanka spoke of the importance of cooperating with SAARC countries. CVE efforts (including counter-narratives) were mentioned by Switzerland and UAE.

Day-to-Day Programme

Sunday, 2nd April 2017

0000 – 2359hrs Hotel Check-in for Speakers & Participants
Venue : Reception, Level 4, Marina Mandarin Singapore (MMS)

1500 – 1830hrs Conference Registration for Speakers & Participants

Venue : Conference Secretariat @ Libra Ballroom Level 1, MMS

1830 – 2100hrs Cocktail Reception & Welcome Dinner
Venue : Pool Garden, Pavilion, Level 5, MMS
Attire : Casual (short-sleeved shirt/polo t-shirt and long pants) and equivalent attire for women

Hosted by : Ong Keng Yong
Executive Deputy Chairman
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Chew Lock Pin
Senior Director
National Security Coordination Centre
Prime Minister's Office
Singapore

❖❖❖

Monday, 3rd April 2017

0630 – 0845hrs Breakfast
Venue : AquaMarine, Level 4, MMS

0815hrs Arrival of guests
Venue : Marina Mandarin Ballroom (MMB)
Level 1, MMS
Attire : Military attire/service dress (jacket with tie and head-dress) for officers; Lounge suit with tie for male and equivalent attire for female civilians

0905hrs All guests to be seated

0910hrs Arrival of Guest-of-Honour

0915 – 0930hrs Introductory Remarks
Shashi Jayakumar
Head, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

Opening Address
Ong Keng Yong
Executive Deputy Chairman
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

0930 – 0950hrs Group Photo-taking (Speakers and Participants only)
Venue : Gemini Ballroom, Level 1, MMS
Attire : Military attire/service dress (jacket with tie without head-dress) for officers; Lounge suit with tie for male and equivalent attire for female civilians

Speakers and participants proceed to Vanda Ballroom, Level 5, MMS after the Group Photo-Taking session for light refreshment before the Ministerial Dialogue. Ministerial Dialogue is a closed-door session for APPSNO Speakers and Participants only.

Coffee Break
Venue : Vanda Ballroom, Level 5, MMS

0955hrs All guests to be seated

1000 – 1100hrs Ministerial Dialogue
Venue : Vanda Ballroom, Level 5, MMS
Attire : Military attire/service dress (jacket with tie without head-dress) for officers; Lounge suit with tie for male and equivalent attire for female civilians

Chairperson : Ong Keng Yong
Executive Deputy Chairman, RSIS, NTU, Singapore

Speaker : Mr K Shanmugam
Minister for Home Affairs and
Minister for Law, Singapore

1100 – 1200hrs Session I: Innovation and Technology
Venue : Marina Mandarin Ballroom (MMB)
Level 1, MMS

Chairperson : John Yong
Adjunct Senior Fellow, CENS, RSIS, NTU, Singapore

Speakers : Simon Moores
Director of Research
Zentelligence (Airads) Ltd
United Kingdom

John C. Mallery
Research Scientist
Computer Science & Artificial Intelligence Laboratory
Massachusetts Institute of Technology
United States

Benjamin Ang
Senior Fellow;
Coordinator, Cyber Programme
CENS, RSIS, NTU, Singapore

1200 – 1300hrs Lunch
During lunch you may wish to change to smart casual attire (long-sleeved shirt without tie) and equivalent attire for women

1300 – 1430hrs Session I: Syndicate Discussions
Venue : Blue Group @ MMB (Capricorn Ballroom)
Green Group @ Aquarius Ballroom
Yellow Group @ Pisces Ballroom

1430 – 1800hrs Perspectivity Challenge
(on-going with coffee break)
Venue : Poolside, Pavilion, Level 5, MMS
Attire : Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Facilitators : Perspectivity Foundation

1800 – 1830hrs Freshen up

1830 – 1900hrs 7th APPSNO Alumni Cocktail Reception
Venue : Vanda Ballroom Foyer, Level 5, MMS

1900 – 2000hrs 7th APPSNO Alumni Distinguished Dinner Lecture:
Innovation & National Security
Chairperson : Joseph Liow
Dean, RSIS, NTU, Singapore

Speaker : Peter Ho
Chairman, URA Board;
Senior Advisor, Centre for Strategic Futures;
Senior Fellow, Civil Service College, Singapore

2000 – 2130hrs Dinner

❖❖❖

Tuesday, 4th April 2017

0630 – 0845hrs	Breakfast	
	Venue	: AquaMarine, Level 4, MMS
0900 – 1000hrs	Session II: Resilience in the Post-Truth Era	
	Venue	: MMB, Level 1, MMS
	Attire	: Smart casual (long-sleeved shirt without tie) and equivalent attire for women
	Chairperson	: Norman Vasu Deputy Head; Senior Fellow, CENS, RSIS, NTU, Singapore
	Speakers	: Ryan Lim Founding Partner; Principal Consultant QED Consulting Pte Ltd Singapore Jakub Janda Head, Kremlin Watch Program; Deputy Director for Public and Political Affairs European Values Think-Tank Czech Republic Janis Berzins Director Center for Security and Strategic Research National Defence Academy of Latvia Latvia
1000 – 1030hrs	Coffee Break	
1030 – 1200hrs	Session II: Syndicate Discussions	
	Venue	: Blue Group @ MMB (Capricorn Ballroom) Green Group @ Aquarius Ballroom Yellow Group @ Pisces Ballroom
1200 – 1430hrs	Lunch followed by Free and Easy (Networking Time) Please change to casual attire (short-sleeved shirt / APPSNO polo t-shirt and long pants and equivalent attire for women) after lunch before the next activity.	

1445hrs	Assemble at Hotel Lobby for Historical Tour Attire : Casual (short-sleeved shirt/APPSNO polo t-shirt and long pants) and equivalent attire for women
1500 – 1815hrs	Historical Tour
1815 – 1900hrs	Light Refreshment Venue : MMB Foyer, Level 1, MMS
1900hrs onwards	Free and Easy (Networking Time) * Dinner is not provided.

❖❖❖

Wednesday, 5th April 2017

0630 – 0845hrs Breakfast
Venue : AquaMarine, Level 4, MMS

0900 – 1000hrs Country Presentation on Homeland Security Management
Venue : MMB, Level 1, MMS
Attire : Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Chairperson : Norman Vasu
Deputy Head; Senior Fellow, CENS, RSIS, NTU, Singapore

Presenters : By alphabetical order starting with host country,
Singapore, Australia, Bahrain, Bangladesh, Brunei and Cambodia

1000 – 1100hrs Session III: Innovation in Terrorism and Counter-Terrorism
Venue : MMB, Level 1, MMS

Chairperson : Shashi Jayakumar
Head, CENS, RSIS, NTU, Singapore

Speakers : Clarke Jones
Director
Australian Intervention Support Hub
School of Regulation and Global Governance Australian National University
Australia

Elaine Pressman
Distinguished Senior Fellow;
Scientific Expert
Netherlands Institute of Forensic Psychiatry and Psychology
Netherlands

Ali Soufan
Chairman and Chief Executive Officer
The Soufan Group
United States

1100 – 1115hrs Coffee Break

1115 – 1245hrs Session III: Syndicate Discussions

Venue : Blue Group @ MMB (Capricorn Ballroom)
Green Group @ Aquarius Ballroom
Yellow Group @ Pisces Ballroom

1245 – 1630hrs Lunch followed by Free and Easy (Networking Time)

1645hrs Assemble at Hotel Lobby
Group transportation is provided to Distinguished Dinner Lecture. Admission to dinner venue is strictly in group.

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

1730 – 1830hrs Distinguished Dinner Lecture: Defense Innovation

Venue : Gemini Ballroom, Level 1, Resorts World Convention Centre, Resorts World Sentosa, Sentosa

Chairperson : Shashi Jayakumar
Head, CENS, RSIS, NTU, Singapore

Speaker : Christopher Kirchhoff
Partner
Defense Innovation Unit Experimental
United States

1845 – 1915hrs Cocktail Reception

Venue : S.E.A Aquarium, Resorts World Sentosa, Sentosa

1930 – 2100hrs Dinner

Venue : S.E.A Aquarium, Resorts World Sentosa, Sentosa

2100hrs Transportation to Marina Mandarin Singapore

❖❖❖

Thursday, 6th April 2017

0630 – 0845hrs Breakfast
Venue : AquaMarine, Level 4, MMS

0900 – 1200hrs Country Presentation on Homeland Security Management (on-going with coffee break)
Venue : MMB, Level 1, MMS
Attire : Smart casual (long-sleeved shirt without tie) and equivalent attire for women

Chairpersons : Damien D. Cheong
Research Fellow;
Coordinator, Homeland Defence Programme CENS, RSIS, NTU, Singapore

Adrian Tan
Deputy Head of Policy Studies, RSIS, NTU, Singapore

Presenters : By alphabetical order,
China, Georgia, India, Indonesia, Japan, Korea, Laos, Malaysia, Myanmar, New Zealand, Norway, Pakistan, Philippines, Spain, Sri Lanka, Switzerland, Thailand, United Arab Emirates, United States and Viet Nam

1200 – 1300hrs Lunch

1300 – 1400hrs Session IV: Innovation in Strategic Communication
Venue : MMB, Level 1, MMS

Chairperson : Damien D. Cheong
Research Fellow;
Coordinator, Homeland Defence Programme CENS, RSIS, NTU, Singapore

Speakers : Gregory Tangonan
Professor; Founding Director
Ateneo Innovation Center
School of Engineering
Ateneo de Manila University
Philippines

Lock Wai Han
Chairman, Media Literacy Council;
Chief Executive Officer, OKH Global Ltd
Singapore

Alvin Tan
Head of Public Policy, South East Asia
Facebook
Singapore

1400 – 1530hrs Session IV: Syndicate Discussions
Venue : Blue Group @ MMB (Capricorn Ballroom)
Green Group @ Aquarius Ballroom
Yellow Group @ Pisces Ballroom

1530 – 1600hrs Coffee Break

1600hrs onwards Free and Easy (Networking Time)
* Dinner is not provided.

Friday, 7th April 2017

0630 – 0845hrs	Breakfast	
	Venue	: AquaMarine, Level 4, MMS
0900 – 1000hrs	Session V: Case Studies	
	Venue	: MMB, Level 1, MMS
	Attire	: Smart casual (long-sleeved shirt without tie) and equivalent attire for women
	Chairperson	: Bilveer Singh Adjunct Senior Fellow, CENS, RSIS, NTU, Singapore
	Speakers	: Antonia Yulo Loyzaga Chairperson International Advisory Board Manila Observatory, Philippines
		Jeff Moss Founder and CEO, DEF CON Communications; Founder, The Black Hat Briefings United States
		Linton Wells II President and Chief Executive Officer Global Resilience Strategies, United States
1000 – 1030hrs	Coffee Break	
1030 – 1200hrs	Session V: Syndicate Discussions	
	Venue	: Blue Group at MMB (Capricorn Ballroom) Green Group at Aquarius Ballroom Yellow Group at Pisces Ballroom
1200 – 1430hrs	Lunch *	
	Venue	: AquaMarine, Level 4, MMS
1430 – 1830hrs	Free and Easy (Networking Time)	

1830 – 1900hrs	Cocktail Reception	
	Venue	: MMB, Level 1, MMS
	Attire	: Smart casual (long-sleeved shirt without tie) and equivalent attire for women
1900 – 1945hrs	11th APPSNO Certificate Presentation Ceremony	
	Presented by :	Joseph Liow Dean, RSIS, NTU, Singapore
1945 onwards	Closing Dinner	
	Hosted by :	Joseph Liow Dean, RSIS, NTU, Singapore

** Notes:*
Participants whom wish to participate in Muslim Friday prayers are to meet at 12 noon at the Conference Secretariat. A chartered bus will ferry participants to and from Sultan Mosque. Lunch will be available at AquaMarine, Level 4, MMS upon returning to the hotel.

List of Guest-of-Honour and Speakers

GUEST-OF-HONOUR

Mr K Shanmugam
Minister for Home Affairs and Minister for Law
Singapore

SPEAKERS

Benjamin Ang
Senior Fellow;
Coordinator, Cyber Programme
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Janis Berzins
Director
Center for Security and Strategic Research
National Defence Academy of Latvia
Latvia

Peter Ho
Chairman, URA Board;
Senior Advisor, Centre for Strategic Futures;
Senior Fellow, Civil Service College
Singapore

Jakub Janda
Head, Kremlin Watch Program;
Deputy Director for Public and Political Affairs
European Values Think-Tank
Czech Republic

Clarke Jones
Director
Australian Intervention Support Hub
School of Regulation and Global Governance
Australian National University
Australia

Christopher Kirchhoff
Partner
Defense Innovation Unit Experimental
United States

Ryan Lim
Founding Partner;
Principal Consultant
QED Consulting Pte Ltd
Singapore

Lock Wai Han
Chairman, Media Literacy Council;
Chief Executive Officer, OKH Global Ltd
Singapore

Antonia Yulo Loyzaga
Chairperson
International Advisory Board
Manila Observatory
Philippines

John C. Mallery
Research Scientist
Computer Science & Artificial Intelligence Laboratory
Massachusetts Institute of Technology
United States

Simon Moores
Director of Research
Zentelligence (Airads) Ltd
United Kingdom

Jeff Moss
Founder and CEO, DEF CON Communications;
Founder, The Black Hat Briefings
United States

Elaine Pressman
Distinguished Senior Fellow;
Scientific Expert
Netherlands Institute of Forensic Psychiatry and Psychology
Netherlands

Ali Soufan
Chairman and Chief Executive Officer
The Soufan Group
United States

Alvin Tan
Head of Public Policy, South East Asia
Facebook
Singapore

Gregory Tangonan
Professor; Founding Director
Ateneo Innovation Center
School of Engineering
Ateneo de Manila University
Philippines

Linton Wells II
President and Chief Executive Officer
Global Resilience Strategies
United States

List of Chairpersons

CHAIRPERSONS

Damien D. Cheong
Research Fellow;
Coordinator, Homeland Defence Programme
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Joseph Liow
Dean
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Ong Keng Yong
Executive Deputy Chairman
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Shashi Jayakumar
Head
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Bilveer Singh
Adjunct Senior Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Adrian Tan
Deputy Head of Policy Studies
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Norman Vasu
Deputy Head;
Senior Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

John Yong
Adjunct Senior Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

List of Participants

AUSTRALIA	**Robert McKinnon** Assistant Secretary Strategic Issues and Intelligence Branch International Security Division Department of Foreign Affairs and Trade Australia
BAHRAIN	**Tareq AlThawadi** Advisor National Security Agency Bahrain
BANGLADESH	**Mejbah Uddin** Director National Security Intelligence Bangladesh
BRUNEI DARUSSALAM	**P.A. Mohammed Saifullah Idris** Ag Director Operations Department Royal Brunei Police Force Negara Brunei Darussalam
BRUNEI DARUSSALAM	**Siti Maszaiwati Haji Zaini** Assistant Director Brunei Research Department Prime Minister's Office Negara Brunei Darussalam
CAMBODIA	**Ro Binike** Chief of International Relations Bureau General Department of Research and Intelligence Cambodia Intelligence and Research Department Cambodia

CAMBODIA	**Duong Uddam** Director of External Operations General Department of Research and Intelligence Cambodia Intelligence and Research Department Cambodia
CHINA	**You Dongxiao** Deputy Director Teaching and Intepretation Translation Division College of Defence Studies National Defence University China
GEORGIA	**Marina Malvenishvili** Deputy Chief Legal Division Cyber Security Bureau Ministry of Defence Georgia
INDIA	**Shri S.M. Sahai** Joint Secretary National Security Council Secretariat India
INDONESIA	**Aryo Aji Dirgantoro** Senior Counter Terrorism Analyst State Intelligence Agency (BIN) Indonesia
INDONESIA	**Wahban** Deputy Director, Analysis Unit; Deputy Foreign Affairs State Intelligence Agency (BIN) Indonesia
JAPAN	**Noriaki Kawamura** Deputy Director 2nd International Affairs Department Cabinet Intelligence and Research Office Japan

KOREA, REPUBLIC OF	**Lee Mihyeon** Deputy Director International Policy Division Ministry of National Defence Republic of Korea
LAO PDR	**Phornmanee Xayasouk** Deputy Chief Intelligence Department Ministry of Public Security Lao People's Democratic Republic
MALAYSIA	**Nazrul Fazami Bin Mohamad** Director Management Services Department National Security Council Prime Minister's Department Malaysia
MALAYSIA	**Meor Syahrizal Azryl** Principal Assistant Director Prime Minister's Department Malaysia
MYANMAR	**Kyaw Zay Ya** Deputy Director Relation Division Special Branch Myanmar Police Force Myanmar
NEW ZEALAND	**Justin Allan** Senior Advisor and Secretary Officials' Committee for Domestic and External Security Coordination (Governance); Strategic Risk and Resilience Panel Department of the Prime Minister and Cabinet New Zealand

NORWAY	**Harald Rasmussen** Head Preparedness and Emergency Response Unit Directorate for Civil Protection and Emergency Planning Norway
PAKISTAN	**Diyar Khan** Joint Secretary National Security Division Pakistan
PHILIPPINES	**Abelardo Pacis Villacorta** Chief Directorial Staff National Intelligence Coordinating Agency Philippines
SINGAPORE	**A Muhd Thauheed** Deputy Commander (Intelligence) Integrated Checkpoints Command (Air) Immigration & Checkpoints Authority Singapore
SINGAPORE	**Nasrath Begam Binte Abul Hassan** Senior Assistant Director Media Relations and Planning Office Ministry of Education Singapore
SINGAPORE	**Vincent Chey Tjun Kit** Assistant Director (Security) Health, Safety, Security & Emergency Preparedness (HSSEP) Department Public Utilities Board Singapore
SINGAPORE	**William Chik Kam Weng** Deputy Director South Asia 1 Branch South Asia & Sub-Saharan Africa Directorate Ministry of Foreign Affairs Singapore

SINGAPORE

Elaine Ee Tze-Yin
National Maritime Sense-Making Group
Singapore Maritime Crisis Centre
Ministry of Defence
Singapore

SINGAPORE

Arthur Fong Hock Siong
Director
Operation Preparedness Division
Infocomm Media Development Authority
Singapore

SINGAPORE

Sherry Foong Poh Chuen
Head, Finance Systems Transformation;
Head, Finance
Ministry of Finance
Singapore

SINGAPORE

Kenneth Gn Jong Bin
Deputy Assistant Chief of General Staff
Operations -Current Operations
Singapore Armed Forces
Singapore

SINGAPORE

Joseph Goh Chun Hwee
Deputy Director
Public Transport Security
Land Transport Authority
Singapore

SINGAPORE

Goh Ing Nam
Program Director
Sensors Division
DSO National Laboratories
Singapore

SINGAPORE

Thomas Goh Toh Chih
Senior Assistant Director
Security & Emergency Planning Office
Ministry of Education
Singapore

SINGAPORE

Gwee Aik Chiong
4 Deputy Director Operations
Singapore Police Force
Singapore

SINGAPORE

Denise Hng Poh Hong
Deputy Director
Emergency Preparedness
Crisis Preparedness Directorate
Joint Operations Group
Ministry of Home Affairs
Singapore

SINGAPORE

Ho Choo Liang
Deputy Director
Jurong Island Security Department
Security Division
Engineering & Operations Group
JTC Corporation
Singapore

SINGAPORE

Wesley Ho Tze Wee
Head
Operations Branch
2nd SCDF Division
Singapore Civil Defence Force
Singapore

SINGAPORE

Kua Choon Jin
Deputy Director (Research)
Police Intelligence Department
Singapore Police Force
Singapore

SINGAPORE

Eddie Liew Wah Yeow
Director (Training)
Centre for Protective Security Studies
Ministry of Home Affairs
Singapore

SINGAPORE

Lena Lim Siew Hwung
Assistant Director
National Service Policy Department
Ministry of Defence
Singapore

SINGAPORE

Lim Swee Keng
Deputy Director (Advisory)
Centre for Liveable Cities
Ministry of National Development
Singapore

SINGAPORE

Lim Weng Kee
Deputy Director (Contingency & Scenario Planning)
Operations Planning & Development
Emergency Preparedness and Response Division
Ministry of Health
Singapore

SINGAPORE

Ian Loe Wai Yew
Director (Cyber Security Monitoring & Response)
Government Technology Agency of Singapore (GovTech)
Singapore

SINGAPORE

Christine Loh Suet Har
Director, Futures & Strategy Division;
Director, Economic Security & Resilience Division
Ministry of Trade & Industry
Singapore

SINGAPORE

Loh Woon Liang
Branch Head
Joint Operations Department
Ministry of Defence
Singapore

SINGAPORE

Douglas Mun Kwok Yeen
Deputy Director
National Cyber Incident Response Centre
Cyber Security Agency of Singapore
Singapore

SINGAPORE

Ng Cher Keng
Director
Airport Economic Regulation & Aviation Security Division
Civil Aviation Authority of Singapore
Singapore

SINGAPORE

Patrick Ng Chun Chow
Senior Assistant Director
Operations Planning Branch
Singapore Prison Service
Singapore

SINGAPORE

Ng Khai Song
Senior Assistant Director, Operations Research;
2 Senior Assistant Director, Intelligence Operations
Intelligence Division
Central Narcotics Bureau
Singapore

SINGAPORE

Raymond Ng Kheng Hong
Assistant Director
Operations Management
Singapore Prisons Service
Singapore

SINGAPORE

Melvern Ong Chin Siong
Assistant Director
Total Defence Engagement
NEXUS
Ministry of Defence
Singapore

SINGAPORE

Rathi Parimalan
Superintendent
Schools Branch West 1
Schools Division
Ministry of Education
Singapore

SINGAPORE

Sean Poh Wee Yong
Vice President
Certis CISCO Security Pte Ltd
Singapore

SINGAPORE

Sim Jim Ho
Senior Deputy Director
Security & Emergency Planning Department
Power System Operation Division
Energy Market Authority
Singapore

SINGAPORE

Paulinhno Soliano
Commander
Special Operations Force
Singapore Armed Forces
Singapore

SINGAPORE

Tan Hoe Koon
Deputy Commander (Intelligence)
Integrated Checkpoints Command (SEA)
Immigration & Checkpoints Authority
Singapore

SINGAPORE

Katie Tan Khai Shuen
Assistant Director
Security Operations Planning
JTC Corporation
Singapore

SINGAPORE

Gregory Tan Siew Hin
Deputy Director
Security and Resilience
Strategy Group
Prime Minister's Office
Singapore

SINGAPORE	**Tan Yoke Cheng** Head Capability Development (National Security) Defence Science and Technology Agency Singapore
SINGAPORE	**Terrence Teo Tsu Tang** Malaysia and Brunei 1 Branch Southeast Asia I Directorate Ministry of Foreign Affairs Singapore
SINGAPORE	**Tok Choon Min** Head Special Investigation Branch Intelligence & Investigation Division Singapore Customs Singapore
SINGAPORE	**Yeo Yee Chuan** Assistant Director Specialised Crime Division Criminal Investigation Department Singapore Police Force Singapore
SINGAPORE	**Peter Yew Chee Seng** Deputy Director National Security Research Centre National Security Coordination Secretariat Prime Minister's Office Singapore
SPAIN	**Felix Jose Alvarez Saavedra** General Secretary Spanish National Police Spain
SRI LANKA	**Ralph Anthony Nugera** General Officer Commanding Sri Lanka Army Sri Lanka

SWITZERLAND	**Jacques Repond** Senior Investigative Officer Swiss Federal Criminal Police Switzerland
THAILAND	**Luejit Tinpanga** Deputy Director Directorate of Countering Transnational Threats Office of the National Security Council Thailand
THAILAND	**Piya Kongkhum** Director Information and Communication Technology Center National Intelligence Agency Office of the Prime Minister Thailand
UNITED ARAB EMIRATES	**Khalifa Altamimi** National Security Specialist National Supreme Security Council United Arab Emirates
UNITED STATES	**Joseph Bradley** Unit Chief Polygraph Unit Federal Bureau of Investigation United States
VIET NAM	**Nguyen Nang Khieu** Department of External Relations General Department of Security Ministry of Public Security Viet Nam

About the Centre of Excellence for National Security

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

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

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

About the S. Rajaratnam School of International Studies

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

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

About the National Security Coordination Secretariat (NSCS)

The **National Security Coordination Secretariat (NSCS)** was formed under the Prime Minister's Office in July 2004 to coordinate security policy, manage national security projects, provide strategic analysis of terrorism and national security related issues, as well as perform Whole-Of-Government research and sense-making in resilience.

NSCS comprises three centres: the National Security Coordination Centre (NSCC), the National Security Research Centre (NSRC) and the Resilience Policy and Research Centre (RPRC).

Please visit www.nscs.gov.sg for more information.

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg