13th ASIA-PACIFIC PROGRAMME FOR SENIOR NATIONAL SECURITY OFFICERS (APPSNO)

NATIONAL SECURITY IN THE AGE OF DISRUPTION

8 – 12 April 2019 | Singapore

Event Report

Organised by

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

With the support of

NSCS NATIONAL SECURITY COORDINATION SECRETARIAT

Report on the Programme organised by:
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University, Singapore
Supported by:
National Security Coordination Secretariat (NSCS)
Prime Minister's Office, Singapore
Rapporteurs:
Nur Diyanah binte Anwar, Cameron Sumpter, Dymples Leong Suying, Pravin Prakash, Romain Brian Quivooij, Jennifer Yang Hui, and Eugene Tan E Guang
Editors:
Teo Yi-Ling
Daniel Prakash

The Programme 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 13th annual Asia-Pacific Programme for Senior National Security Officers (APPSNO) was held at Marina Mandarin Singapore from 7 – 12 April 2019. Organised by the Centre of Excellence for National Security (CENS) with support from the National Security Coordination Secretariat (NSCS) in the Prime Minister's Office (PMO), the programme's theme was National Security in the Age of Disruption".

Speakers from a range of nations, including the United States, Australia, the United Kingdom, Japan, Hong Kong, Finland, and Singapore shared their expertise and experiences on the following topics:

1. **Drivers of Disruption** – rethinking politics in a time of unprecedented challenges, a changing geopolitical landscape, and the weaponising of artificial intelligence to create propaganda.

2. **Disrupting Violent Extremism** – trends in radicalisation and mobilisation dynamics, cultivation of neo-Nazi groupuscules in an online context, and managing terrorism, extremism, and exclusivism in Southeast Asia.

3. **Cybersecurity and Disruption** – the current cybersecurity threat landscape and international efforts to address cyber threats, the geopolitics of technology, safety and security of autonomous and semi-autonomous systems, and Singapore's strategy in creating a resilient and trusted cyber environment.

4. **Technology and Society** – digital platforms disrupting the labour force, models of platform cooperativism, the impact of automation on trade policy, upskilling workers, and the governance of Chinese society with AI technologies.

5. **Case Studies** – climate change as a national security threat, the regulation of cross-border cyber-intrusions, the impacts to society and work from new technology, and universal basic income as a solution.

The event brought together senior national security officers from the Asia Pacific and beyond to Singapore for a week of thought-provoking and relationship-building conversations. Sixty-three participants from 23 countries gathered to discuss the challenges of emerging national security concerns. Foreign participants were joined by their Singaporean counterparts from various government ministries and agencies.

In keeping with the Programme's theme, Minister for Foreign Affairs Dr Vivian Balakrishnan opened the programme by highlighting the changing parameters of national security challenges.

Beyond the panel presentations and breakout discussion groups, international participants delivered country presentations, providing a concise overview of their respective state's national security threats and responses. Further enriching the programme was a distinguished dinner lecture by Sir John Scarlett KCMG OBE, former Chief of the British Secret Intelligence Service, who outlined several key requirements for effective organisational leadership in disruptive times.

Presentation Summaries

Session 1: Drivers of Disruption

Rethinking National Security in Times of Planetary Politics: Challenges and Opportunities

Sabine Selchow, *Research Fellow, University of Sydney, Australia*

Understanding contemporary disruptions today requires states to question their thinking behind the premises, principles, and conceptual lenses that underpin the *raison d'etre* of their political structures and institutions. States are unwilling to give up traditional concepts in national security like war and peace, but are themselves disrupting national security conversations by assigning new understandings to fit zombie institutions.

Geopolitical Drivers of Disruption

Nick Biseley, *Head, School of Humanities and Social Sciences, Professor of International Relations, LaTrobe University, Australia*

The resurgence of geopolitics in the region is disrupting international relations in the Asia-Pacific. The evolving world view of China and United States and their corresponding role in security affairs, will disrupt the relative peace that the region has enjoyed for the past

four decades. This competition among the great powers may result in both economic and military conflict.

Computational Propaganda: How Artificial Intelligence is Being Weaponised to Manipulate Populations

Sean Gourley, *Founder and CEO, Primer, United States of America*

Human dominance in the cognitive space will be quickly eroded by machines over the next decade. Machines are able to take on tasks that humans are biologically unable to do, or do at speeds and volumes that humans are unable to match. This will cause a seismic impact on society and the role that humans play within it.

Distillation

1. State institutions are often not equipped with the tools or mandated to deal with disruption, causing state responses to disruption to sometimes be ineffective and inadequate.
2. The emergence of technological drivers of disruption is often linked to the ever-shifting geopolitical dynamics and competition among states.
3. Disruption to national security is not limited to new sources such as AI, but can also come from traditional sources like geopolitical competition.

Session 2: Disrupting Violent Extremism

Current Trends in Terrorist Radicalization and Mobilization in the West

Lorenzo Vidino, *Director, Program on Extremism, Georges Washington University, U.S.A.*

Western Europe has been at the forefront of the global Jihadist outbreak since it began in 2013. The peak of the crisis was reached in 2016-2017 when attacks occurred or were uncovered on a regular basis. While the situation appears to have calmed down, challenges related to the prosecution of returning foreign fighters and their rehabilitation raise complex issues.

National Action, Atomwaffen Division and Cultures of Neo-Nazi Transnational Activism

Dr. Paul Jackson*, Senior Lecturer in History, Faculty of Education and Humanities, University of Northampton, U.K*.

National Action and Atomwaffen Division demonstrate how violent British far-right groups can be. Such organisations come into existence quickly and then disappear. They interact with each other and provide members and sympathizers with the ideological inspiration that can ultimately lead to violent attacks.

Proscription of these groups show that the British authorities take this threat very seriously.

Managing Terrorism, Extremism and Exclusivism

Rohan Gunaratna, *Professor of Security Studies, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

Southeast Asia is not immune from the Islamic State (IS) threat. Pledges of allegiance to IS's leader made by heads of terrorist groups based in Southeast Asian countries show that the region is vulnerable. A key requirement is for governments to counter the threat in cyberspace, as IS has been successful in radicalising individuals and communities through social networks.

Distillation

1. Motives that explain why individuals have radicalised in Western Europe are not limited to a single factor. IS introduced significant changes in logistical aspects of terrorist activities such as funding. Profiles of individuals that IS recruiters managed to enroll are also more diversified than what they used to be during the two previous decades.
2. Organisations such as National Action and Atomwaffen Division confirm that terrorist threats in the U.K. are not limited to Jihadist groups. As proven by attacks or projects of attacks against left-wing MPs, individuals who are strongly influenced by the beliefs and convictions of these groups represent a

security risk.

3. The Internet has proven to be a powerful tool used by IS to spread propaganda, raise funds, convince individuals to join the organization in the Middle East or carry out attacks in their home countries. This explains why Southeast Asian governments should focus their efforts on the cyberspace, in addition to kinetic efforts in the physical world.

Session 3: Cybersecurity and Disruption

The Global Cyber Threat Landscape – Overview and Future Trends

Andrew Grotto, *William J. Perry International Security Fellow, Stanford University, United States of America*

Concerns over safety, security, and privacy lie at the nexus of the cyber threat landscape. Recommendations were made on how governments should adopt an integrated approach to digital governance, establish bilateral and multilateral digital governance cooperation fora on smart devices, and set reasonable objectives. Private enterprises and academia should also play a part in adopting an integrated approach to managing safety, security, and privacy risks associated with smart devices.

Disruptive Cybersecurity Technology

Danit Gal, *Assistant Professor, Global Research Institute, Keio University, Japan*

The discussions over disruptive cybersecurity technology should take into account geopolitical considerations and the nature of technology. The disruptive capabilities of technology are exponential, and no technology is entirely safe and secure. Cybersecurity and safety need to increase in importance as technology progresses.

Singapore's Cybersecurity Strategy

Gwenda Fong, *Director (Strategy), Cyber Security Agency, Singapore*

Singapore's increasing reliance on Information and Communications Technology mean that Singapore is a prominent target for cyberattacks. It is impossible for states to guarantee that there will be no future successful attacks because cyber attackers need only one successful attack out of many to cause disillusionment with the state; but cyber defenders are required to be impregnable all the time.

Distillation

1. There is a part for everyone in society to ensure cybersecurity. Academia, government, society, and

private enterprises need to work together to create a safe, secure, and resilient ecosystem.
2. Technology does not replace the need for skilled human operators. There is as much a need to invest in training human capital as there is in infrastructure.
3. The increasing concentration of technology development in American and Chinese hands may create new threats to national security on a geopolitical basis.

Session 4: Technology and Society

Managing Digital Disruptions for Sustainable Digital Labour and Regional Peace

Jack Linchuan Qiu, *Professor, School of Journalism and Communication, Chinese University of Hong Kong, Hong Kong*

A rapidly growing section of the global workforce is now termed ‘digital labour’, because of its support for businesses operating on emerging technologies. These technological disruptions are leaving workers in unstable conditions with uncertain futures, threatening social fault lines. Promoting cooperative models of labour organisation may counter this by ensuring sustainable livelihoods and establishing resilient communities.

Technology, Economic Security and Social Impact: The Art of Craft and Competitive Public Policy

Shihoko Goto, *Deputy Director for Geoeconomics, Senior Associate for Northeast Asia, Asia Program, Wilson Center, USA*

Global trade policy is often perceived in zero-sum terms, whereby national governments fear losing out to transnational competitors. Such analysis emphasises deficits in the trading of goods, and tends to ignore the importance of exchange of services. Job losses blamed on competition from foreign labour markets are more accurately explained by advancements in automation. Relevant skills training is essential to keep pace with technological evolution.

AI-powered Governance in China: Implications for Asia Pacific Countries

Sabrina Luk, *Assistant Professor, Public Policy and Global Affairs, Nanyang Technological University, Singapore*

Emerging technologies, such as artificial intelligence, are increasingly being deployed to address urban inefficiencies and establish smart cities based on big data. China, leading the way, has deployed combinations of networked CCTV cameras, facial recognition technology, and vast databases of individual information to iron out societal wrinkles such as jaywalking. While

these strategies may present effective solutions, they risk significantly eroding privacy and human dignity.

Distillation

1. Technology has substantially disrupted existing business models. While consumers benefit from improved efficiency and greater choice, workers suffer from uncertainty and insecurity. If governments fail to protect livelihoods and employment sustainability, injustice-based grievances will likely lead to social fractures and potential violence.
2. Human societies have been affected by technological evolution for centuries, but the speed and breadth of change the world is now witnessing may be unprecedented. Growing complexity increases the likelihood of misinterpreting causality and laying blame where it may be undeserved. Straightforward explanations can offer political expedience, but greater nuance will produce more effective solutions to pressing problems.

3. Governments seeking to exercise control over their citizens will eagerly embrace emerging technologies that facilitate comprehensive command. People may even welcome increased privacy intrusions if they mean greater efficiency, security and potential reward. However, policing citizens through advanced surveillance systems

and harsh control measures may put a nation on a dependent path toward totalitarianism. Any remnant of a social contract would be rendered meaningless.

Session 5: Case Studies

Climate Change as a National Security Issue

Angel Hsu, *Assistant Professor, Social Sciences (Environmental Studies), Yale-NUS College, Singapore*

Climate change poses existential risks to all aspects of national security, and is increasingly viewed as a threat multiplier. Governments should enhance existing policies to reflect this growing threat. Concerted efforts in understanding the socio-economic nexus of climate change (e.g. impact to economies and migration) can help alleviate the consequences of climate change.

Intrusion Across Borders

Jennifer Daskal, *Associate Professor of Law, American University, Washington College of Law, United States of America*

Limitations in the international cyber regulatory system have resulted in inadequate regulation of cyber sovereignty. The formulation of new norms for the current international system of cyber sovereignty are needed in

an era where below-the-threshold cyber-based intrusions are increasingly frequent. Regulations providing enhanced powers and capabilities to governments should, however, be tempered with considerations of cyber ethics and privacy.

Practical and Innovative Ways of Enhancing Inclusive Economic Development and Resilience in the Digital Knowledge Economy

Olli Kangas, *PhD, Program Director, The Strategic Research Council at the Academy of Finland, Professor of Practice, Department of Social Research, University of Turku, Finland*

According to an OECD study released in April 2019, the middle class is being squeezed out of the new digital economy. Governments should rethink how innovative social policies can be implemented to minimise the risks the digital economy posits to society and national security. Pilot studies and experiments on basic income by some countries have been proposed as a solution in addressing social and national security risks.

Distillation

1. Governments and institutions should view climate change, cyber sovereignty and economic development as integral to national security and mitigate potential vulnerabilities to safeguard stability and enhance public trust.

2. Climate change, for instance, is increasingly viewed as a threat multiplier to national security, whereas a lack of innovative social policies and tools to tackle rising income inequality and unemployment could threaten social cohesion and unity of nation states.
3. In order to tackle these challenges, there is a need to enhance existing policies and regulations, both on an international and domestic level. Cyber regulatory systems have to be updated, and new cyber norms are increasingly crucial in an era of below-the-threshold cyber-based intrusions.

Lunch Lecture

Sign of the Times? Disruptions, Discontents, and Directions of the International Order

Joseph Liow, *Dean, College of Humanities, Arts and Social Science*, *Nanyang Technological University*, *Singapore*

The world is being pushed deeper into geopolitical uncertainty. A key vector is the downturn in Sino-U.S. relations that have manifested in an escalating trade war, and which threaten to undermine global stability and economic growth. The security concerns over Huawei are only the beginning of a long-drawn challenge that will have a range of implications on global stability. The challenge for states is formulating a response to these extremely fluid conditions.

Distillations

1. The U.S.-China rivalry has materialised in the form of a technology war that has proven disruptive, and is likely to continue to shape the global order.
2. While there has been a lack of solid evidence for security concerns over Huawei, contextual evidence may point to some grounds for concern.
3. There is the need to include technical points of view when discussing regional geopolitical issues.

Lunch Discussion: National Security and Disruption – A Singapore Perspective

Society, Narratives, and Disruption

Norman Vasu, *Senior Fellow and Deputy Head, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

States use the power and utility of narratives as a way to organise societies. These narratives can feed into a greater narrative, with this serving as the foundation and the *raison d'etre* of the state: a series of mini stories that contribute to the meta-narrative. Singapore is no exception, having constructed a meta-narrative that emphasises how security should not be taken for granted.

Cybersecurity and Homeland Defence in Disruption

Benjamin Ang, *Senior Fellow, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

Forces of disruption can only be fought with more disruption and a better understanding of what citizens and markets want. Disruption should however not be done for its own sake, but to better square security with growth, and innovation with timely regulation. States should therefore not fear disruption, but perhaps should disrupt their own legacy problems before they become victims of disruption.

Terrorism / Radicalisation

Shashi Jayakumar, *Senior Fellow and Head, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

In Singapore, social media now plays a central role in processes of radicalisation, which have increased in tempo and involve younger antagonists who are more difficult to engage through de-radicalisation programmes. We are witnessing an increased diversity of extremist views.

Distillation

1. States should not take the framing and consumption of national narratives for granted, and find new ways to retell founding stories to avoid it becoming a tired trope.
2. States should not shy away from disrupting or reforming their own processes, because maintaining such processes opens up avenues for other actors, including the private sector, to provide services.
3. Social media's impact on terrorism and radicalisation is great. Social media brings with it a greater diversity of extremist views, and makes it easier for individuals to become radicalised, with little contact with an organised terrorist group.

Distinguished Dinner Lecture

Strategic Leadership: Managing Disruption for National Security – Lessons from Personal Experience

Sir John Scarlett KCMG OBE, *former Chief of the British Secret Intelligence Service, United Kingdom*

In a time where terrorism and non-state actors increasingly dominate the security landscape, combined with the evolving nature of threats and the speed of change, effective organisational leadership is now more crucial than ever. Apart from personal qualities of integrity, professionalism, and accountability, effective leadership is demonstrated by assembling an optimally-

balanced support team comprising a range of personalities, experience, and skills. This is critical for formulating strategic directions, and generating timely responses to crises.

Distillation

1. Leadership is often about adapting to sudden changes, particularly scenarios that one may not necessarily be trained for. This requires leaders to adapt, adopt new strategies and learn new skills, and this is even more crucial in these disruptive times of sharp learning curves.
2. Leaders must be seen to have integrity, accountability, and fully committed to the optimal performance of the organisation. A leader must be supported by a capable leadership team that does not suffer from groupthink. It may freely discuss and disagree in private, but must then consolidate and outwardly project a cohesive message.
3. The difference between this period of geopolitical uncertainty over previous periods is the speed at which change is occurring, creating greater uncertainty.

Opening Address

Ambassador Ong Keng Yong
Executive Deputy Chairman, RSIS, NTU, Singapore

Ambassador Ong Keng Yong opened the 13th Asia-Pacific Programme for Senior National Security Officers (APPSNO) by highlighting the timely significance of the programme's theme, 'National Security in the Age of Disruption'. Rapid technological developments are driving opportunities for innovation but also produce complexity and uncertainty. Global change and disruption bring unique national security challenges that require multidisciplinary perspectives and fresh thinking. The five panels curated for the Programme run the gamut of pressing contemporary issues, and the surrounding discussions should push boundaries and generate creative responses.

Ministerial Address

Dr Vivian Balakrishnan
Minister for Foreign Affairs, Singapore

1. Human nature has never changed, but technology is evolving at such a pace that societies are struggling to contend with the implications. The world has reached a level of interconnectedness where ideas circulate globally in real time,

creating a sense of dislocation in the way we engage each other, organise our societies, and mobilise our communities. Such transformation brings social and political disruption with profound implications for national and global security. Three key and current concerns are polarisation, radicalisation, and cyber threats.

2. Globalisation and technological progress have brought many benefits, but there is an overwhelming feeling that the promised fruits have not been distributed quickly or evenly enough. Anxiety has set in throughout the world and an ‘anti-elite’, inward looking, fractious mood now permeates politics everywhere. The right and left are drifting further apart. More ominously, societies are witnessing a hollowing of the political centre and middle class. Breakdown in domestic consensus has led to disruption in the liberal rules-based order, whereby countries fear change and competition.

3. Radicalisation leading to indiscriminate ideological violence remains a critical issue. Today’s frontline is in cyberspace, where terrorists and political opportunists spread propaganda, recruit followers and coordinate attacks. New tools such as live streaming offer gruesome opportunities to connect audiences with violence. The unregulated online sphere is also now plagued by dangerous falsehoods

seeking division and mistrust, which can have severe consequences for our social fabric.

4. Cyber threats are increasingly sophisticated and asymmetric in nature. Several countries, including Singapore, have recently experienced cyber incidents which not only risk immense financial losses, but threaten interconnected critical infrastructure, weaken justice systems and erode public trust in government. Besides cyber-attacks, advances in information technology have also increased our vulnerabilities, through cyber-espionage and the spread of disinformation. We must remain vigilant regarding the risk of foreign entities seeking to influence domestic politics through the open cyberspace.

5. Singapore is intent on addressing the social disruption brought about by the technological revolution. The priority is investing in people, both through relevant skills training and ensuring a social security trampoline that enables people to bounce back and keep up with the challenges of the future. Singapore is looking to pass new legislation to act decisively against online falsehoods. Media literacy will be a crucial ingredient, as will ongoing multi-stakeholder engagements to promote interfaith dialogue and social cohesion.

Session 1: Drivers of Disruption

Rethinking National Security in Times of Planetary Politics: Challenges and Opportunities

Sabine Selchow, *Research Fellow, University of Sydney, Australia*

1. States have different views of, and are affected differently by disruptive activity. This difference can be seen through how they utilise modern thinking about issues like growth and progress, ideas of knowledge production, the concepts of societies as national containers, and decision-making in controlling the effects of disruption over time and space.

2. Despite the efforts expended to understand and discuss issues, thinkers always seem to be one step behind the curve, and do not seem to fully grasp the nature of the problems. Some problems like conflict do go away, but come back again after a short while.

3. Not only are people failing to go deep enough in analysing the issues, but they are also failing to appreciate the need to shift perspectives in finding new ways forward. An example is the issue of climate change, where there is enough knowledge that it is a phenomenon brought on by

humans, but states seem to think that the effects can be controlled or tamed.

4. A second line of thinking is needed to ensure that institutions are well equipped to deal with new and complex problems. An example of this is the European Union's 2016 Global Strategy. The strategy recognises that developments around the world today are complex in nature, and the conceptual language used to explain such phenomena causes polarisations among populations. Old political theories like power may not adequately provide answers for these global developments. The strategy therefore calls for new conceptualisations of what national security means, and take into account new geographies and non-traditional security issues such as human security.

5. States need a paradigm shift to deal with disruption. This can be done by both expanding and shifting the loci of its institutions and how it looks at national security, and understanding the alternative conceptual language used globally to understand problems. Further, states could build on and question existing discourse, and shift the making of strategic assessments from an integration approach (globalisation) to a more dynamic understanding (planetary politics).

Geopolitical Drivers of Disruption

Nick Biseley, *Head, School of Humanities and Social Sciences, Professor of International Relations, LaTrobe University, Australia*

1. The assumptions underpinning the regional order are increasingly being undermined by a rising China. Among these assumptions is the view that China will become more liberal politically after its economic liberalisation, and that great power competition had ended. These assumptions were borne out of the liberal triumphalism that permeated among neo-liberals after the end of the Cold War.

2. The Asia-Pacific region is seeing the return of great power politics because the great power bargain agreed by the United States and China in the 1970s is breaking down. There is little to suggest that the United States and China are ready to compromise. Chinese policy has shifted from a hide-and-bide position to one that is abrasive and seeks to recast regional security architecture. The United States for its part has not been clear about its goals and its commitment to the region, but has made remarks that has inflamed Chinese sensitivities.

3. The vectors of competition between China and the United States will take place on many levels,

and many of these stem from old rivalries which in turn exacerbate the threats to the region. Among these are the political resolution over the status of Taiwan, and the role of the Chinese as a global leader in standard-setting for new growth areas such as artificial intelligence and cyber issues.

4. There are four possible trajectories that great power rivalry between China and United States may take. First and the most optimistic of these trajectories is for China and the United States to renegotiate or re-establish a grand bargain that each state compromises some of its positions and in turn reduce conflicts in the region. Second is the creation of an Asia where everything is integrated with some level of Chinese technology, and increasing the profile of Chinese influence in the region. Third, there may be full spectrum competition between China and the United States; this competition may include standards and policy positions, and the security concerns may be addressed militarily. The fourth trajectory envisions a new Cold War between China and the United States where both states decouple economically to reduce integration for security reasons.

Computational Propaganda: How Artificial Intelligence is Being Weaponised to Manipulate Populations

Sean Gourley, *Founder and CEO, Primer, United States of America*

1. At this point in time, artificial intelligence (AI) is not quite there yet, and there remains a number of challenges to get it right. There is a lot of hype over AI, and understanding it properly requires a sense of reality where the technology actually is, its potential applications, and its limitations.

2. AI is a branch of machine learning that seeks to optimise the independent execution of processes by way of algorithms learning from data fed to them. The study of artificial and neural networks is where most of the research has been focusing largely on for the past four to six years, driven by the quest to enable machines to conduct "deep learning" by themselves.

3. "Deep learning" has revolutionised AI through greater understanding of voice, image recognition, and the generation of language. The development to "deep learning" from "shallow learning" emerged about 15 to 20 years ago. "Deep learning" allows neural networks to function on multiple hidden representations to

create an output, and these representations do not have to be determined by humans.

4. AI has developed tremendously in the last few years, and is now able to generate photographs and text that seem realistic and plausible to the general public. These subjects in these photographs and the attribution of text are derived from image and text databases, to depict a convincing story.

5. Knowledge of this technology can be used for nefarious purposes, such as the creation of computational propaganda. Computational propaganda can potentially be used to disrupt critical national functions like influencing the outcomes of elections, or to cause economic panic by interfering in the operation of stock markets. Adversarial states may see computational propaganda as a means of conducting information operations for the purpose of influencing outcomes in other states.

6. As AI becomes more pervasive in our modern day lives, the need for good judgement by humans becomes more valuable and important to distinguish fact from fiction.

Syndicate Discussion

1. Issue: Unknown unknowns undermine risk assessment. Modern thinking does not adequately address the issue of unknown unknowns. It fails, for example, to consider the consequences of risks over the long run. Risk itself is a modern development; a way of dealing with uncertainties of the future by making decisions now about issues or events that could possibly happen. Modern thinking therefore proposes dealing with risks by encouraging more knowledge management. Unknown unknowns, however, undermine this type of risk assessment because the interaction between drivers of disruption is more complex than is already known. Academics and policymakers should therefore attempt to better understand the interplay between forces of disruption.

2. Issue: "Globalisation", "planetary", and the blurring concept of boundaries. "Globalisation" is often associated with open markets and neo-liberal ways of thinking. By contrast, "planetary" refers to going beyond the global, and is not restricted to economic globalisation. It suggests that the planet has boundaries, and that there is a need to rethink these boundaries and its social relations. For example, "national borders" is becoming increasingly irrelevant, and it is becoming difficult for leaders within the European

Union to prevent the influx of refugees into their states. Thus, the blurring of boundaries will have implications for security practitioners such as the law enforcement and the military, as well as how regional organisations address issues affecting them.

3. Issue: Regulation in artificial intelligence (AI) and disinformation. There is the need to regulate the virality of online information and AI, which hitherto can be programmed for quick distribution and to attract as much attention as possible. However, it would be difficult to agree on regulatory standards on AI that would be accepted by all parties at the local, regional or international levels. It could also lead to the creation of an inflexible apparatus that might quash dissenting views. It is largely not in the digital platforms' interests to take into account national security concerns, or be regulated. Therefore, states need to develop relevant capabilities and awareness with regard to AI and its potential use in disinformation, as well as work with the relevant technology companies. This can include encouraging media literacy courses in schools or online, to counter disinformation from a young age.

4. Issue: Is a "Terminator scenario" involving autonomous defence systems, weapons and robots possible? There is wide acceptance in the US that AI is a major component of the third offset

strategy. The offset strategy refers to a set of military innovations that allow a country to take decisive advantage on its competitors. Therefore, mastering AI would be a powerful deterrent preventing potential enemies from going to war with the US. This may suggest that the use of autonomous defence systems, weapons and robots is only a matter of time, and close to becoming reality.

5. Issue: Strategic relations between China and the West. The main driver of Chinese economic success is China itself. China is still a largely internally-driven economy, just like the US. Chinese political leaders are aware that their economic success was largely borne from their own domestic economy. Simultaneously, the *realpolitik* between the US and China may lead to decreased levels of trade and investments between the two states, as each side sees the other in an increasingly militarised manner. While business with China is crucial for many Western institutions, it may be even more difficult to have a mutually beneficial economic relationship in the near future.

Distillation

a) Boundaries in national security are becoming increasingly blurred, and there is a need to

consider potential security threats from angles that may have not been previously considered.

b) The digital space may continue to be weaponised for disinformation purposes. It is therefore important to conduct active surveillance to monitor potential threats.
c) AI technology moves at a fast pace, and may raise legal and regulatory issues in the near future which have not yet been considered.
d) Western countries' perceptions of China may have been plagued by distrust and suspicions of hegemonic intentions in global politics and economy.

Session 2: Disrupting Violent Extremism

Current Trends in Terrorist Radicalization and Mobilization in the West

Lorenzo Vidino, *Director, Program on Extremism, Georges Washington University, U.S.A.*

1. An unprecedented surge of radicalisation happened in Western Europe between 2013 and 2017. With more than 5000 individuals identified as foreign fighters and a Muslim population of 25 million people, Europe is the region that has produced the highest percentage per capita of

foreign fighters. The number of arrests is equally significant, as around 1000 individuals were arrested by security services throughout the continent. 70 attacks have also been carried out during this timeframe.

2. Four levels of analysis are required to understand why this wave of radicalisation occurred. The first level is geopolitical: the conflict in Syria was a major driver. The second level is socioeconomic, with feelings of discrimination and marginalisation explaining to a certain extent why some men and women resorted to violence. The third level is psychological. From that perspective, the quest for meaning and identity turned out to be a key factor. The fourth level involves charismatic recruiters who influenced individuals or small groups of people.

3. Typologies of attacks show differences with the pre-Islamic State (IS) era when terrorist acts were initiated by al-Qaeda (AQ). Out of the 70 attacks carried out between 2013 and 2017, only two relied on a central organisation that trained perpetrators, gave them instructions and sent them to Western Europe. About 30% of the attacks were carried out by individuals who had limited links with IS. By contrast, 70% of these terrorist acts were implemented by people whose

connection with the mother group was limited to ideology.

4. Among the trends that have been emerging since 2013, the expanded crime-terror nexus stands out. A very large number of attackers have a criminal past. These people often continue their criminal activities after embracing a radical ideology. Terrorism financing has also been characterised by the fundraising of small amounts of money by attackers or their accomplices. In addition, the profiles of radicalised individuals reveal that the percentages of women, converts, young people and individuals with mental issues are higher than before the rise of IS on the international scene.

5. Legal and security challenges make it difficult for countries' national authorities to counter this threat. In particular, many returning foreign fighters cannot be charged due to the lack of evidence of their involvement in violent activities in Iraq/Syria. In addition, the surge of right-wing extremism and the difficulties encountered in reintegrating radicals will pose significant problems for the years to come.

National Action, Atomwaffen Division and Cultures of Neo-Nazi Transnational Activism

Dr. Paul Jackson, *Senior Lecturer in History, Faculty of Education and Humanities, University of Northampton, U.K*.

1. Fascism is understood by historians as the attempt of a national or a racial group to transcend liberal democracy or political pluralism. Many neo-Nazi groups identify as fascist. Neo-Nazism refer to a subset of fascism that blends National Socialism with contexts and ideas that appeared after 1945. A cultic milieu is a space offering access to taboo ideas, a sense of the higher, and seekership, as well as radical critiques of the mainstream. Transnational activism points to the exchange of ideas and the fostering of a sense of community across borders.

2. National Action (NA) was a neo-Nazi group founded in 2013 by young militants Ben Raymond and Alex Davies. Their objective was to create a movement that would be more ideologically authentic than other groups operating in the U.K. at the time. Its first high-profile actions were to target a female MP, Luciana Berger, and to stage provocative demonstrations. Propaganda texts issues by NA such as *Strategy and Promotion* idealised a youthful ‘style’ and called for revolution.

3. NA was eventually proscribed in December 2016 under terrorism legislation. However, this did not prevent other similar or follow-on groups to be created such as NS131, Scottish Dawn, and System Resistance Network. From September 2017 these groups were also proscribed and more members were arrested. In 2018, several former militants of NA were tried. This included Jack Renshaw, a far-right activist who plotted to murder Labour MP Rosie Cooper.

4. Atomwaffen Division (AD) was one of the groups with which NA used to be networking. AD claimed to offer an 'autonomous Fascist lifestyle'. Its members developed a neo-Nazi approach based on the ideas of American activist James Nolan Mason. Similar to NA, AD targeted university campuses and idealised white supremacist terrorists such as Dylan Roof and Anders Breivik. It now operates in a more clandestine way, often online, and includes activists located in Canada.

5. Groups such as NA and AD create an extremely violent narrative and idealise a fascist revolutionary transformation. They both also typify a wider, transnational trend to develop cultic forms of neo-Nazism that offer a deeper sense of meaning and mission. These organisations pose some threats of developing terrorist plots. The risk of violence often comes

from fringe members who are driven to violent acts by a combination of ideological and non-ideological factors.

Managing Terrorism, Extremism and Exclusivism

Rohan Gunaratna, *Professor of Security Studies, S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

1. Three significant processes and events define the threat environment in Southeast Asia. First, the Southeast Asian landscape is fused with the global landscape. This means that events that happen in distant regions such as the Middle East have a direct impact on Southeast Asian countries. Second, IS has gradually expanded from the Middle East to Western countries, Africa and Asia. Third, the group has shifted from the physical to the virtual domain.

2. The radical Indonesian cleric Aman Abdurrahman was able to convince many of its followers in Southeast Asia that terrorist attacks were legitimate. His arguments were that dying in the course of an attack would bring the attacker closer to God and that his/her sins would be forgiven. Abdurrahman's role was instrumental in convincing the leaders of 63 groups and cells active in Southeast Asia to pledge allegiance to the head of IS.

3. IS was able to radicalise a greater percentage of people in Southeast Asia than al-Qaeda (AQ) managed to. For instance, the percentage of Indonesians believing in the virtues of the Caliphate and Sharia law rose by 10-15%. This surge is largely due to the emergence of IS on the international scene from 2014, as well as the influence gained by the group in the following years. It is very likely that the base of IS supporters in Indonesia will continue to expand.

4. Face-to-face interviews conducted with convicted terrorists in Indonesia, Malaysia and the Philippines revealed that almost all of these individuals were radicalised online. In particular, Facebook is the most popular platform used by IS to spread extremist content and build up networks in Southeast Asian countries. After a while, radicals tend to shift from Facebook to the encrypted application Telegram.

5. There is no clear separation among Indonesian, Malaysian and Filipino terrorist networks. Historically, prominent members of these networks have travelled extensively, lived in different Southeast Asian countries, and influenced each other.

6. The bigger terrorist threat does not come from returnees. It emanates from individuals who did not travel to Iraq/Syria but have been radicalised

online. Overall, the counter-terrorist responses of governments in Southeast Asia has been effective. However, the IS threat will remain persistent in the years to come. As such, countries need to invest resources in both the physical and cyber spaces to counter this threat.

Syndicate Discussion

1. Issue: Areas which should be focused on in post-Islamic State (IS) era. Dynamics of mobilisation explaining how radical actors interact with each other should remain a key focus. Good practices and lessons learnt in prevention and rehabilitation also require further investigation. Much research being done currently focuses on best practices when terrorists are released back into society, but also on why some individuals become extremists, while other groups of people remain immune to radicalisation. Additionally, how online propaganda can continue to radicalise should also be studied. The themes currently found online are of trials and tests, and how the current state of IS is one of temporary defeat. Also, how radicalised netizens are following such propaganda should be monitored, considering the fact that many are interested in the concept of jihad - and not the IS per se.

2. Issue: Which is easier to detect and disrupt - well-organised attacks or the “lone wolf” attacker?

Several attacks that involved clear structures of command and control have been thwarted by security services. Such plots are easier to detect as they leave traces related to funding, online communications, weapons and explosives. This creates opportunities for interceptions and pre-emptive arrest, unlike attacks carried out by “lone wolves”. The number of attacks where levels of command and control were limited or non-existent is actually very low, but these attacks have been the most lethal. The 2016 attacks in Nice and Orlando (87 and 50 people killed, respectively) have shown how deadly such operations can be.

3. Issue: Monitoring Southeast Asian foreign fighters returning from Iraq and Syria. In the Philippines, the number of locals who joined IS remains very low. In the case of Indonesia, about 600 to 700 people had travelled to Syria and Iraq. 400 of these individuals are tracked by intelligence agencies. One of the biggest challenges in Southeast Asia is the lack of a joint task force focusing exclusively on foreign fighters. Regional governments need to cooperate and coordinate intelligence to track those who have joined IS that hail from Southeast Asia, and those who have returned. In addition, countries like Indonesia must build credible rehabilitation programmes and improve capacity-building efforts, to effectively manage the returnee population.

4. Issue: Countering the growing presence of extreme-right groups. There are many extremist groups in the United Kingdom that have attempted to gain legitimacy and go mainstream, by leveraging on political arguments against minorities, such as the Muslim community. This can be observed on social media platforms, as such extremist groups look to spread their online content quickly and widely. The role of civil society and regulation on social media platforms is vital in creating awareness, and ensuring such hate messages are not normalised. For example, Facebook changed its policy on content associated with white nationalism after the 2017 Charlottesville attack.

Distillation

a) Analysing terror attacks since the emergence of IS, from various angles, can provide useful insights into terrorists' motivations, strategies and networks. Security practitioners must therefore continue to keep abreast of evolution in their modus operandi and ideology.
b) The online space continues to be weaponised for jihadist purposes. Efforts must therefore be made to monitor cyberspace and prevent it from being used for terrorism.
c) Governments in the Southeast Asian region must beef up their counter-terrorism strategies, and

have streamlined and coordinated efforts at monitoring the activities of returnees.

d) The fall of the IS caliphate does not mean the elimination of radicalisation. Efforts must be present to look out for the next iteration of radicalism, such as the far-right threat.

Session 3: Cybersecurity and Disruption

The Global Cyber Threat Landscape – Overview and Future Trends

Andrew Grotto, *William J. Perry International Security Fellow, Stanford University, United States of America*

1. Devices have been updated on a piecemeal basis, mainly to retain their basic functionality. This approach however may cause unintended consequences to the safety and security of the equipment, and heighten privacy concerns of the user.

2. Governments should adopt an integrated approach to digital governance that aligns risk management initiatives across privacy, security and safety. Different arms of the United States government like the White House, Department of Homeland Security, and Congress should work

together to create an open and transparent process, in order to solicit industry and civil society input regarding risk management initiatives.

3. Governments should establish bilateral and multilateral digital governance cooperation fora on smart devices, and set reasonable objectives. The forum should focus on joint learning about the intersection of safety, security and privacy risks in smart devices, with an initial emphasis on critical infrastructure. The forum should develop mechanisms for information sharing about these risks, and serve as a platform for exchanging ideas and experiences on approaches to managing these risks.

4. Enterprises should adopt an integrated approach to managing safety, security, and privacy risks associated with smart devices. Corporate boards (or their governance equivalents) should demand this approach, develop performance metrics, and hold executives accountable. Vendors and customers, along with trade associations, should develop voluntary frameworks for managing safety, security and privacy risks throughout the life cycle of smart products.

5. Scholars should develop joint research agendas that integrate safety, security and privacy. Legal, engineering, social science, and policy oriented

scholarship in academia and civil society reflects these risk domain stovepipes. There are rich traditions of scholarship and civic engagement on safety and privacy, and a growing body of cybersecurity scholarship. There is also a strong base of literature on comparative regulatory affairs. Scholars must bring these bodies of work together into a coherent research agenda.

Disruptive Cybersecurity Technology

Danit Gal, *Assistant Professor, Global Research Institute, Keio University, Japan*

1. There are a few considerations to take into account when discussing cybersecurity technology.
    a. First, it cannot be discussed separately from geopolitics, and attempting to dissociate technology discussions from geopolitics dilutes the understanding of why technology wars happen. Powerful countries will fight over and use powerful technologies, and while this is not a new phenomenon, the use of technology has scaled the possibility of conflict upwards.
    b. Second, virtual weapons create a situation where states can find themselves potentially at war perpetually, because technology creates a scenario where attacks are constantly happening while

being invisible. This is opposed to a traditional situation where there are pauses in conflict.

c. Third, while technology is an essential tool, the increasing complexity of technologies mean that the more complex the system used, the more vulnerabilities it has.

2. Most of the critical information infrastructure technology is increasingly coming from the United States and China, and traditional sources like Germany and Japan are increasingly becoming marginalised. In part, the United States-China trade war is about how Chinese technology is progressing, and how they have supplanted American companies that were manufacturing in China.

3. China is reverse engineering a lot of technology from Germany and Japan, and builds new products on these platforms, enabling their new products to be compatible with the existing systems, rather than being stuck on proprietary hardware produced by states like Japan and Germany. Although the reverse engineering approach brings opportunities for states that do not want to change out the whole infrastructure, it also brings risks if reverse engineering is done incorrectly and exposes the whole system to more vulnerability.

4. Disruptive cybersecurity technology today follows four main trends: first, the possibility of automated or augmented virtual attacks; second, the possibility of attacks on the hardware used in critical infrastructure; third, how users are making it easier for hackers to surveil by sharing their location unquestioningly; and fourth, how vulnerabilities are becoming complex as systems become more complex.

5. Operators need to be smarter and more capable than the system that they are operating, rather than delegating decision making to the machines. Known as the "automation paradox", systems may fail in unexpected ways, which require more skilful human handling to recover. Organisations should therefore invest more in training and equipping human capital with the right skillsets to operate the complex systems they are investing in.

<u>Singapore's Cybersecurity Strategy</u>

Gwenda Fong, *Director (Strategy), Cyber Security Agency, Singapore*

1. Singapore's cyberspace is vast and complex, and encompasses many different sectors both nationally and internationally. On the national front, Singapore's concerns with regard to

cyberspace include its designated critical information infrastructure, emerging technology, its public sectors, and defence, security and intelligence gathering apparatus. Singapore cooperates with other states internationally through its CERT capabilities and its security agencies, and is an active participant in the development of norms and international law for cyberspace.

2. Cybersecurity is an existential issue for Singapore, like physical security. Singapore has recently created a new pillar – digital defence – under its total defence framework, signifying the importance that the Singapore government has placed on cybersecurity. This is especially so given the ambitions of Singapore to become a Smart Nation.

3. There are four key areas in Singapore's cybersecurity strategy: first, to build resilient infrastructure; second, to create a safer cyberspace; third, develop a vibrant cybersecurity ecosystem; and fourth, to strengthen international partnerships.

4. Building a resilient infrastructure is critical for Singapore because essential services rely on information and operations technology, and cyberattacks on critical information infrastructure can disrupt Singapore's economy and society. To

this end, Singapore has updated its Cybersecurity Act, created a critical information infrastructure protection programme, conducted cybersecurity exercises with both the private and public sectors, and incorporated a security-by-design framework for government systems.

5. Singapore aims to create a safer and more trustworthy cyberspace by emphasising the collective responsibility of cybersecurity by all users, including the government, businesses, and the community. To do this, Singapore has rolled out various initiatives, such as the National Cybercrime Action Plan, the National Cybersecurity Awareness Campaign, and the GoSafeOnline Platform.

6. Singapore sees the creation of a strong cybersecurity ecosystem as an engine for economic growth, and an imperative to ensure that Singapore's cyberspace is trusted and secure. The development of both manpower and industry are both important pillars in creating this strong ecosystem.

7. Singapore is a responsible global citizen that has an interest in international discussions on cybersecurity and cooperation among states. Cyber threats do not respect borders, so technology development, information sharing, and operations need to be coordinated to ensure

the spill-over effects of cyberattacks are minimised.

Syndicate Discussion

1. Issue: International cyber norms. It has been challenging for Association of Southeast Asian Nation (ASEAN) member states to agree on what international cyber norms should entail. The Cyber Security Agency (CSA) of Singapore has taken the initiative to get ASEAN member states to understand and agree to a set of cyber norms, and work towards its adoption, as well as enhancing cyber cooperation in the region. This has been a largely challenging task due to existing geopolitical issues between member states, and might not be resolved any time soon.

2. Issue: Preventive measures against cyber-attacks. Under the Cyber Security Act 2018, Singapore's CSA has the power to formally designate systems as critical information infrastructure (CII), and oblige CII owners to put in place processes to safeguard against cyber-attacks. Regulations include regular risk, security, and vulnerability assessments. While the CSA is responsible for prescribing the method for preventive measures, sector owners take care of the actual implementation suitable for the needs of the sector.

3. Issue: International scrutiny on Huawei could ironically benefit it. Huawei is responding to feedback from international regulatory bodies by fixing its products much more quickly than before. Political boycotts by several countries concerned about Huawei's close links with the Chinese state also fail to hurt it. For example, while the United States has advised allies not to use Huawei products and technology, Washington did not provide them with viable alternatives. Therefore, even though most countries agree Huawei may not be the safest option, private or state-owned companies located in these countries continue to sign deals with Huawei. The company is also signing more agreements with other countries, and operating in the rural areas of the same.

4. Issue: Avoiding cyber risks require leadership from the top. While governments have developed distinct processes and institutions over the decades, some arms of the government have little consideration of and expertise in matters of privacy and security. It has also been challenging to get corporations to think about security, and how it interplays with other domains. Therefore, there is the need for senior management and C-suite executive-level engagement to understand the importance of security and privacy - especially in the public domain.

5. Issue: Have we reached a point of complexity where it is almost impossible to teach people about technology? Technological systems are becoming increasingly complicated, but it does not mean we should forego teaching citizens to familiarise themselves with them. While there is a growing technological gap amongst the older generation, the youth and technologically-savvy are almost digital and AI natives. Understanding how basic systems work (such as protocols and data packets involved with emailing) is essential. Therefore, there is a need to ensure how such technology is accessible to as many people as possible.

Distillation

a) National cybersecurity agencies are complex ecosystems that deal with all dimensions of cyber security, from training to regulations and international cooperation.
b) Strong leadership is needed to develop sound processes and institutions for cybersecurity.
c) Information-sharing among countries for cybersecurity issues must be enhanced through better engagement and international treaties.
d) The effectiveness of Washington's strategy in pressuring other countries not to rely on Huawei is doubtful at best. Engagement through open-source and co-sharing in developing common

standards might therefore be a more suitable way of relating to Huawei, moving forward.

Session 4: Technology and Society

Managing Digital Disruptions for Sustainable Digital Labour and Regional Peace

Jack Linchuan Qiu, *Professor, School of Journalism and Communication, Chinese University of Hong Kong, Hong Kong*

1. Digital platforms are disempowering working people. Jobs are becoming more precarious, workers are getting paid less, and receive less societal respect. Data is extracted from the labour process not to build local infrastructure and improve lives, but to create global tax-avoiding monopolies.

2. The world of artificial intelligence has become bifurcated between the United States and China, whose technology companies are structured in similar ways and employ the same ultra-capitalist model of development, based on excessive exploitation. However, the fault lines of the future will not only form between nations but also within our respective societies – between the working people who do not own technology and the trans-national capitalist classes who have the whole gamut of technological tools at their disposal.

3. Critical information infrastructures at the national level are increasingly owned and managed by multinational corporations. They are driven by achieving global supremacy rather than establishing sustainable and prosperous living conditions for the masses. Grievances stemming from this dynamic threaten social fault lines and by extension, pose genuine risk for national, regional, and even global security.

4. One way of empowering workers and ensuring fairness of outcome is through the promotion of platform cooperativism, which combines the well-established co-op movement with contemporary technological tools. The roughly four-year-old platform co-op movement now represents a global ecosystem of start-ups, working with emerging technologies to build democratically governed and worker-owned online businesses that generate long-term jobs and greater prosperity. In addition to individual gains in salary, service and quality, workers can take ownership of companies and build resilience to weather the storm of disruption.

5. Investing in the worker-owned digital economy, and thereby redirecting value away from global corporations back into communities, will lead to more peaceful and prosperous societies. The worldwide digital commons can become a transnational public sphere of trustworthy

information and shared knowledge, which is locally distributed and sustained through social and cultural values.

Technology, Economic Security and Social Impact: The Art of Craft and Competitive Public Policy

Shihoko Goto, *Deputy Director for Geoeconomics, Senior Associate for Northeast Asia, Asia Program, Wilson Center, USA*

1. In recent years, the world has witnessed a growing trend among governments, particularly in the United States and Western Europe, to move away from transnational trade agreements. This apparent protectionism is reflected by the anti-globalisation movement, which is driven not by concerns of trade specifics but largely by imbalanced social dynamics at play in a range of nations.

2. The current United States government perceives itself as disadvantaged among existing international trade rules. The Trump administration is fixated on the nation's trade deficit in goods, but a more nuanced inspection of outcomes suggests this may be a simplification. Over the past 20 years, the United States has seen its trade surplus of services increase substantially vis-à-vis all major economies, including China.

3. Job losses blamed on unfair trade deals are more connected to advancements in automation than international transfers of labour. In 2018, humans made up 71% of the global labour force, compared with machines at 29%; however, according to the World Economic Forum, this will be reversed by 2025, when robots are expected to work more hours globally than humans. Nations must upskill their workforces, not to compete with machines, but to contribute to rapidly changing models for production mechanisms and service delivery.

4. An example of an evolving industry is the automobile market, which is undergoing more changes than most sectors. Executives at certain major companies no longer refer to their products as vehicles or cars, but as ‘mobile entertainment units’ or ‘mobile transportation modules’. Functions other than driving will be increasingly promoted as driverless technology makes travelling safer and more energy efficient.

5. Trade deals are not necessarily a source of trade deficits and social instability. Much of the perceived issue is the result of increased automation. When balancing the value of trade deals with other nations, it is important to look at both goods and services, as well as different sections of the national economies in question.

AI-powered Governance in China: Implications for Asia Pacific Countries

Sabrina Luk, *Assistant Professor, Public Policy and Global Affairs, Nanyang Technological University, Singapore*

1. Driven by artificial intelligence (AI), robotics and the Internet of Things, so-called ‘smart cities’ are developing apace across the world, as governments seek to address growing urban challenges. Roughly one thousand smart cities are currently being established in various nations, half of which are located in China. The Chinese government has stated its goal is to become a global leader in AI technologies by 2030, and by 2020 the nation will have implemented over 600 million AI-powered CCTV cameras throughout its territory.

2. A useful case study for understanding the extent to which China is realising its AI objectives is the way the government is dealing with traffic infringements. Authorities in major cities have now employed AI enhanced cameras with up to 7 million pixels of resolution to capture photos of pedestrians crossing roads illegally. Through advanced facial recognition technology, images of jaywalkers are matched with municipal police databases, and their photos and personal information are displayed on giant LED screens at intersections.

3. Traffic transgressions are also reported to the culprit's workplace, which is deemed to be particularly effective when a jaywalker is employed at a company classified by the authorities as 'civilised', which may place limits on the person's career prospects. To further name and shame, municipal police post jaywalker photos on social media, where they may be kept online for 3-5 years.

4. Data strongly suggests this approach reduces the incidence of jaywalking. However, observers are concerned police may exercise unfair discretion, and that the system represents an unjustified invasion of privacy. Furthermore, mistakes raise the issue of algorithmic accountability – that is, who or what is responsible when innocent citizens are wrongly accused of infringements.

5. AI relies heavily on big data to build its intelligence, and while this emerging technology can bring benefits to society, it also presents substantial risk. Basic principles and guidelines to mitigate societal harm are crucial. Fundamentally, AI should be employed in ways consistent with respect for human life, values and dignity.

Syndicate Discussion

1. Issue: Cultural attitudes towards privacy and social responsibility. There are currently on-going

experiments running in China, Germany and Japan on attitudes towards privacy and how it might be influenced with the use of AI in governance. Societal acceptance of privacy may be deeply linked to its culture. In Japan, for example, there is little need for naming and shaming because societal responsibility is deeply imbedded in the Japanese culture. Notions of privacy, though, also change with time and context.

2. Issue: China's social credit system. The social credit system was founded on the idea to categorise people into different grades (very poor, below average, average, good and excellent) according to their social behaviours and activities. Such a scoring system has become accepted in first-tier Chinese cities such as Shanghai. However, it raises three important issues. First, whether digital scores represent exactly who individuals are. Second, the nature of algorithm used by the government to differentiate "good" and "bad" citizens. Third, whether individuals are able to defend or prove themselves, should their scores not reflect their social behaviours accurately.

3. Issue: Efficacy of intergovernmental organisations. Intergovernmental organisations such as the World Trade Organisation (WTO) consist of states that vary in economic standing,

priorities and levels of development. This diversity may impede the effectiveness of the organisation as a whole, as there would be different interests and alliances formed. An example can include when China and Taiwan joined the WTO; there were hopes the former would play by the rules of international world order, but this has largely not panned out.

4. Issue: Domestic issues should be given more attention. Challenges on the bilateral, regional or international fronts may be important, but practitioners should pay attention to domestic issues as well. For example, one major challenge for many countries is how regime succession is becoming increasingly unpredictable. The election of leaders such as U.S. president Donald Trump had resulted in major changes not only with international engagement, but also domestically. Issues such as polarisation within society should therefore be given more attention.

5. Issue: Growing sense of alienation emerging in many countries. Alienation refers to a sense of exclusion, extreme frustration and marginalisation. Those who feel alienated turn to communities which they can identify with; those they perceive as being able to understand their pain and encourage them to fight back. Alienation can affect individuals no matter their profile; it has as much to do with income inequality as other

factors such as religiosity or ethnic identity. Therefore, policymakers and researchers should be analysing data comprehensively to come up with suitable policy prescriptions, rather than only focusing on income inequality and social injustice as the main reasons for missed economic opportunities and possible social unrest.

Distillation

a) China's social credit system has raised many questions related to its approach, its overall effectiveness, and the impact it will have on relations between individuals and the government.
b) There is a need to conduct deeper research into the links between AI in governance, and its impact on society as a whole.
c) Political changes within a state can have drastic effects on both domestic and international politics and national security.
d) Alienation and polarisation within society can be the result of an intersection of factors. Policymakers should not be biased in only focusing on specific factors when prescribing policy recommendations.

Session 5: Case Studies

Climate Change as a National Security Issue

Angel Hsu, *Assistant Professor, Social Sciences (Environmental Studies), Yale-NUS College, Singapore*

1. Governments are increasingly classifying climate change as a threat multiplier to national security. The Pentagon has issued reports which identifies climate change as a threat multiplier, highlighting the immediate and long-term threats that climate change poses to the United States' national security.

2. Key environment threats as a result of climate change include ice melt, sea ice loss and rising sea levels. A warming climate, for instance, could cause seawater volumes to expand and ice over land to melt, both of which will result in a significant rise in sea levels. Impacts due to climate change include a loss in biodiversity and declining levels of human heath (e.g. deteriorating levels of air quality due to air pollution; lower crop yields due to increasing temperature anomalies).

3. There is an urgency amongst governments and academics in respect of understanding the socio-economic nexus of climate change – how the impact of climate change could significantly and adversely impact the national and global economy, and also exacerbate refugee immigration patterns. For instance, research into the recent surge of Central

American migrants into the United States has shown that many migrants are in fact climate refugees, driven to trying to enter the United States because the cycles of their traditional farming livelihoods had been impacted by unpredictable weather patterns.

4. Climate change is also an increasing threat to organisations with large fixed investments. An example of such organisation directly facing threat would be the military. A physical dimension of climate change threat to national security includes the vulnerability of military bases in the United States to recurrent flooding, drought, desertification, wildfires, and thawing permafrost. There is now an exigent effort in the United States to measure, protect and evaluate various policies in trying to bring together research on climate change-related risks and national security vulnerabilities.

Intrusion Across Borders

Jennifer Daskal, *Associate Professor of Law, American University, Washington College of Law, United States of America*

1. The increasing capacity of states to reach across borders via cyber-enabled means has raised questions about the efforts by states to reassert sovereign control. The unresolved nature of legal and policy questions, and norms to govern such actions impact state responses to below-the-threshold cyber-attacks. The international cyber regulatory system

does not adequately and fully categorise such actions, nor does it attempt to regulate them.

2. A recent example of cross-border cyber intrusion was seen in 2018, where a U.S. Cyber Command operation temporarily shut down the servers of the St. Petersburg-based Internet Research Agency (IRA) in November 2018. This was in retaliation for the IRA's electoral interference in the U.S. Presidential Election of 2016. This action was categorised as defensive (i.e. defending against an intrusion on U.S. elections) and offensive (i.e. the shutdown caused actual physical damage to property), and was deemed to be an appropriate and proportionate response to the IRA's interference.

3. Election interference via information warfare does not constitute the use of force under international law. Neither does it violate the traditional rule of law regarding non-intervention, as information warfare is non-coercive in nature. The targeted audience of disinformation in a country is free to ignore false information they receive online. Nation states, however, can take countermeasures to limit information warfare efforts via methods including criminal prosecutions (e.g. the United States has prosecuted certain IRA-related individuals), diplomatic tools, and continued responsive efforts to disinformation.

4. Cross-border, cyber-enabled action on data servers located in a third-party country (e.g. U.S. action on Microsoft's Ireland servers in 2018) could face limitations under international law. Non-obligatory consent by the third-party country could throw up obstacles, especially in counter-terrorism efforts. For instance, seeking to shut down ISIS servers based in multiple countries would require informed consent from the countries.

5. Law enforcement efforts to access data across borders have been enhanced by legislation in some countries. For instance, Australia's Assistance and Access Bill 2018 gives added powers to the Australian government to compel telecommunication companies to build intercepting technologies.

<u>Practical and Innovative Ways of Enhancing Inclusive Economic Development and Resilience in the Digital Knowledge Economy</u>

Olli Kangas, *PhD, Program Director, The Strategic Research Council at the Academy of Finland, Professor of Practice, Department of Social Research, University of Turku, Finland*

1. New production modes in the digital economy (e.g. the digitalisation of products and services) lead to increasing social risks such as rising income inequality and growing unemployment. Increasing automation and digital replacement of

human employment have contributed to uncertainty in societies globally. Concerns over growing unemployment and an expanding precariat require innovative ways to tackle social challenges.

2. The digital economy has also impacted the middle class. The latest OECD Report in April 2019 has recommended that governments do more to implement social policy interventions to assist the middle class. New models of social protection are needed in the digital knowledge economy to meet challenges in financing social protection in the digital age.

3. Governments and institutions should view sound social policy as integral to national security in the way armed forces are integral towards the national security of a nation, and mitigate vulnerabilities to nations' socioeconomic stability. This would go towards enhancing public trust in governments and social institutions.

4. One idea which has gained traction from various governments is the concept of basic income. An experimental pilot study on basic income was conducted in Finland under the auspices of the Prime Minister’s Office of Finland. The objective of the experiment was to evaluate if basic income was a practical and innovative solution to enhance social protection. However, preliminary

findings from Finland's pilot study on basic income demonstrates that basic income faces the similar challenge of financing as other forms of social protection. The full report from the pilot study is due to be released in late-2019.

5. The European Union has pledged to review social policies on the digital economy. Recommendations in the European Union's 'social fairness package' seeks to guarantee people in full-time employment, as well as self-employed workers, access to social protection in the digital and platform economy. Governments should also increase social investment in education (e.g. digital skills) and life-long learning. The facilitation of social dialogues, where different aspects of society are brought together (e.g. employers, employees, elites) can help to devise possible solutions for the digital economy.

Syndicate Discussion

1. Issue: Experiments are context-specific. Experiments on Universal Basic Income may work in one country, but not in another. Most experiments are based on sample sizes that may not be generalizable across contexts. In behavioural studies, significant effects might usually only be observed after two to three years - thus it may not be wise to implement policies based on initial findings before carrying out

comprehensive longitudinal studies. Each society should find its own solutions to challenges they may be facing based on studies grounded on their unique contexts.

2. Issue: Society's support for the basic income project. Support for the basic income project depends on how it was framed to the larger society. For example, in one survey, about 70% of Finnish people who took part considered basic income a positive development. When asked if they would still support the project if the amount given to every person was reduced to 700 euros per month (SGD 1066,) and if additional sources of revenue should be taxed at 45%, only 30% of respondents indicated they would still support the project.

3. Issue: Identifying and countering cyber-attacks. Malicious action in cyberspace is particularly difficult to deal with. First, there is the issue of attribution i.e. determining with certainty who is responsible for the hostile act. Second, the nature of the response must be appropriate and proportional. In this regard, cooperation between states and international organisations is key in countering these threats. As an example, the international community should come together and collectively sanction the Russian interferences in the 2016 U.S. election and the 2017 French presidential election.

4. Issue: Measuring the impact of disinformation campaigns on society. It is necessary to distinguish between traditional information campaigns involving troll farms, and efforts to magnify specific types of content from other operations focused on stealing sensitive information and releasing it to the public. The former could be observed during the 2016 U.S. election, while the latter applied to the 2017 French presidential election. Measuring the effect of such actions on citizens is extremely difficult, as different variables have to be taken into account.

5. Issue: Challenges in removing of online radical content. Challenges persist in the taking down of online terrorist material. Firstly, it is impossible for technology companies to remove all radical content within a short period of time. Secondly, surveillance efforts by the security practitioners themselves may be hampered if these companies become over-enthusiastic in removing radical content – including groups or accounts set up to monitor online activities. This would also affect parties feeding counterterrorism messages onto online platforms, as they might find their content being removed as well.

6. Issue: Difficulties addressing climate change. First, while the technology needed to address

climate change is available (for example, renewable energies, electric vehicles, systems to remove carbon dioxide from the atmosphere, et cetera), a major impediment is the lack of political will. Many governments have little incentive to address climate change. Second, parties seeking to solve the problems may often be the ones to contribute to it. This may include, for example, states dependent on certain manufacturing industries even though they require better air or water quality. Third, there is no effective global central authority to address climate change issues. Lastly, current generations often assume future generations will have the technology and tools to deal with warming temperatures and climate changes.

Distillation

a) Climate change will make natural resources become incredibly scarce, and therefore there is a need to explore alternatives while minimising trade-offs.
b) More often than not, there needs to be regional or international cooperation in addressing issues which affect many parties, such as climate change or disinformation.
c) There is a need to get greater buy-in from the government and citizens to run longitudinal studies which may affect overall livelihoods, such as the basic income project.

d) Policy responses and solutions to issues concerning the state and society (whether it is regarding climate change or basic income) have to be context-based, and tailored to meet respective needs.

Lunch Lecture

Sign of the Times? Disruptions, Discontents, and Directions of the International Order

Joseph Liow, *Dean, College of Humanities, Arts and Social Science*, *Nanyang Technological University*, *Singapore*

1. A series of destabilising trends over the last couple of years have contrived to place the prevailing international political and economic order under increasingly heavy stress. The world is witnessing a disconcerting downturn in Sino-U.S. relations that threatens to undermine global stability and economic growth.

2. The appointment of Donald J. Trump as the president of the U.S. has upended not only U.S. domestic politics, but also its approach to international affairs. Trump has engaged in personalised politics, reaching out to his constituents via microblogging site Twitter and filling his cabinet with neoconservatives who think like him. Politically speaking, there is now a case of small groups making big decisions in the U.S., with wide implications on both the country and the world.

3. Internationally, Trump has engaged in unrelenting offense measures against China, especially by

triggering a trade war. Within his administration, there is a bipartisan consensus on how to deal with China, most likely due to the common desire to push China further. For example, even the speaker of the U.S. House of Representatives, Nancy Pelosi, who is known for her anti-Trump stance, had commended the administration of its handling of the trade war.

4. The trade war has manifested itself as a technology war, contrary to Trump's original intention, which was to bring jobs back to the U.S. Central to this technology war is Chinese multinational telecommunications equipment and consumer electronics manufacturer, Huawei, which has been under intense scrutiny for allegations of espionage. The security concerns of Huawei, however, is a matter of debate. Defenders of Huawei argue that there has not been direct evidence of the company engaging in espionage, thus far.

5. Contextual evidence, however, may be a good reason for security concerns over Huawei: Firstly, Chinese investment and foreign companies are allowed to appoint government officials to their boards. Secondly, 80% of Chinese technology companies are state-owned enterprises, which sees heavy investment by the Chinese government. Thirdly, it is legislated that Chinese

technology companies have to cooperate with the government.

6. Most indicators suggest that the U.S.-China rivalry will be long-drawn and will take a toll on global stability. Moreover, even as dialogue ensues between trade negotiators, voices in Washington and Beijing continue to raise the stakes, making room for manoeuvring increasingly limited.

Discussion

1. Issue: Internal reviews on policy towards Huawei. Many countries around the world are conducting their own internal reviews in formulating policy as regards Huawei. Most are concerned over creating an infrastructure which affords China the option of using it to access data anytime it chooses to do so. For example, Papua New Guinea has contracted Huawei to run its underground cables, which made Australia concerned about interference to its submarine cables. While there is no evidence of China intercepting communication through Huawei cables, there are perceptions that this is possible.

2. Issue: Involving technical input in geopolitical discussion. There is a lack of input of the technical aspects in discussions on regional geopolitical issues. Having two ecosystems will be disastrous

in terms of leading to safety hazards, inconvenience, and creation of multiple vulnerabilities. While it is politically feasible to pressurise Huawei, it is not advisable from the technical point of view. From the industrial point of view, it is also difficult not to engage with Huawei due to its technical capabilities that have been adopted around the world.

Lunch Discussion: National Security and Disruption – A Singapore Perspective

Society, Narratives, and Disruption

Norman Vasu, *Senior Fellow and Deputy Head, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

1. The use of narratives helps to construct the idea of a state, and creates a shared value system through the construction of a narrative arc. This narrative arc can be created by the use of chosen mini-stories, with each imbuing a critical and coherent piece to the meta-narrative.

2. There may be different interpretations to the narratives and which narratives are chosen. This

may cause narratives to be contested among the populations. An example how the British public views Brexit, with some believing in the narrative that Europe has stolen the country away, while others believe that the United Kingdom is better off being part of Europe.

3. Singapore emphasises three main mini-stories in its oft-mentioned meta-narrative of Singapore's vulnerability and how the status quo should not be taken for granted.
    a. First of these is the Japanese invasion of the then-British colony in 1942. In this story, Singapore's vulnerability is highlighted, with a secondary message that Singapore should not depend on others for its security.
    b. The second story is how Singapore obtained its independence as the unlikeliest of states. The narrative claims that independence was unplanned and foisted onto Singapore; that it was a place with no natural resources, and only human resources; and that it was left to fend for itself.
    c. The role of the race and religious riots in the 1950s and 60s is the third story. Despite only having human capital, Singapore's racial harmony is not a natural occurrence, and preserving this

status quo should not be taken for granted.

4. This narrative often faces challenges from the creeping fault-lines among Singaporeans, such as immigration and culture wars between liberal and conservative factions. Disinformation and fake news will further stress the narrative, and create disruptions to the narrative.

5. Narratives are not static, and can be disrupted in the following ways: first, the coherence and fidelity of the narrative can be lost by not having lived through the experience; second, the nature of how trust is formed has changed from authoritative to peer sources; third, there may be mental exhaustion from the public from a narrative being oversold; and, fourth, notions over the concept of citizenship may have evolved from a rational concept to one that has more emotional overtones.

6. While states cannot readily change the national narrative, the emphasis can be altered to avoid the fatigue associated with the overemphasis of a singular narrative. For example, Singapore's emphasis on vulnerability can be tweaked to emphasise its resilience instead.

Cybersecurity and Homeland Defence in Disruption

Benjamin Ang, *Senior Fellow, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

1. Digital disruption is the change that occurs when new digital technologies and business models impact the value proposition of existing business. Examples of technology disrupting businesses can be found in areas of Fintech, where Android Pay and Apple Pay exist without owning a bank, and ride and home sharing platforms such as Uber, Grab and Airbnb have dominated without owning physical assets.

2. Technology itself can also disrupt how humans live, such as disrupting decision-making through the use of artificial intelligence, and the sharing of news without broadcasting, through the use of social media platforms.

3. Disruption typically happens when an incumbent has a legacy to overcome, and is saddled with unsavoury decisions to change its policies, and a low barrier for a disruptor to provide the solution for this unwillingness to change.

4. The Cybersecurity and Homeland Defence Programme is concerned about technology-driven disruption, specifically attacks on disruptors and disruption of attackers. Conflict in

cyberspace should not be seen as an act of war, and adversaries can be destroyed without firing a shot. Examples of attacks on disruptors include attacking platforms, and providing faulty data to artificial intelligence to negatively influence outcomes. Smart cities may also come under threat, especially with smart homes and cars.

5. Attacking disruptors is possible because start-ups typically prioritise growth over security, and seek to push the boundaries of regulation in search of breakthrough innovation. Cyber attackers are also disrupting themselves through the development of new tools, new services, and the use of disinformation and influence operations. These new disruptive tools include the use of botnets, selling hacking tools as a service, and selling intelligence products obtained through cyber means.

6. To combat risks from disruption, states need a paradigm shift to become disruptors themselves. This includes understanding and being unafraid to trial new technology, embracing new models of operation, and understanding and changing the shortcomings in government systems, before getting disrupted.

Terrorism / Radicalisation

Shashi Jayakumar, *Senior Fellow and Head, Centre of Excellence for National Security (CENS), S Rajaratnam School of International Studies, Nanyang Technological University, Singapore*

1. Shortly before 9/11, a number of individuals linked with Jemaah Islamiyah (JI) were apprehended under the Internal Security Act (ISA) in Singapore. With direct links to al Qaeda, this group had serious jihadist intentions, including a possible attack on an MRT station frequented by US servicemen, among other targets. All of the JI-linked suspects were put through a de-radicalisation programme, which for this cohort had a very high success rate, of roughly 85 per cent.

2. However, the situation in Singapore has evolved. Since the mid-2000s, social media has played a crucial role in the radicalisation of those arrested in Singapore, some of whom have little or no linkage to organised terrorist groups. The speed of the radicalisation process has increased, from around two years among the JI generation to roughly nine months today. The average age has dropped, and so too has the success rate of rehabilitation efforts, as the new generation appears more difficult to de-radicalise.

3. At least two Singaporeans attempted to heed the call of the late ISIS leader al-Adnani, who told those who could not make it to Syria to try to conduct attacks at home, yet no plot has been successful. One individual who made it to the Caliphate appeared in a propaganda video in 2017, making all kinds of threats. Two individuals with a particular hatred of Shi'a travelled to Yemen to support the fight against Houthi, while a particularly interesting case involved a Singaporean who was caught while preparing to travel to Syria to fight against ISIS with Kurdish militia.

4. Violent extremism today is complex and has a significant transnational element. The assailant who murdered 50 people in two New Zealand mosques appears to have travelled extensively. International recruits have joined a range of conflicts, and even switched between them, such as from the Ukraine to Syria and Iraq. When we look back on this period, social media will be a key common denominator, as will the prevalence of a perceived persecution complex and a quest for meaning.

Discussion

1. Issue: Radicalised individuals are also interfacing with offline terror groups in addition to online material. While there is material online that may

cause an individual to be radicalised, there is evidence to suggest that some of the first and second generation of ISIS fighters were also in part groomed by offline terror groups to fight for the caliphate. There is a trend however toward individuals being radicalised solely through the publications available online.

2. Issue: The response of states to cyberattacks should be based on attribution, not severity. There is a need to consider both factors of attribution and severity in tandem. The need for attribution is largely political, especially so when a cyberattack is severe enough to warrant a state response. While NATO has declared that Article 5 on collective defence applies to cyberattacks, NATO has not clearly defined the threshold that it considers to be a cyberattack on another state. Therefore, even if there was proper attribution, states need to consider if the cyberattack has passed the threshold where a response is needed or feasible.

3. Issue: The input from recruitment agents in processes of online self-radicalisation. Over the past 6-7 years, online propaganda – predominantly from ISIS – has conveyed messages of empowerment, redemption, and a quest for meaning in life. However, a number of

recruitment cases will have involved personal grooming, which may also take place offline.

Distinguished Dinner Lecture

Strategic Leadership: Managing Disruption for National Security – Lessons from Personal Experience
Sir John Scarlett KCMG OBE, *former Chief of the British Secret Intelligence Service, United Kingdom*

1. Leadership is often about adapting to sudden changes, particularly scenarios that one may not necessarily be trained for. The British intelligence service, for example, is necessarily a small one and officers often work in and lead very small teams. An unfortunate side-effect of this is that one is often not equipped to lead the organisation itself. This requires leaders to adapt, adopt new strategies and learn new skills.

2. In the early 2000s, the intelligence community was coming to terms with the reality of a post 9-11 world, where terrorism and non-state actors increasingly dominated the security landscape. This was a sharp divergence from dealing with the threats of the Cold War, which required a sharp learning curve and a willingness to adapt one's understanding of security threats to the new environment. The 2005 London Attacks exemplified this change as the intelligence

service had to adjust to the idea that citizens born in the UK could be radicalised and become suicide bombers.

3. The Secret Intelligence Service (SIS) also has had to develop a relationship with the media despite its traditionally and often necessarily low-profile nature. However, there was a growing public interest in the secret service. Coupled with the evolving nature of threats, which calls for a more active, supporting role from the public, this interest meant that a careful balance had to be struck between secrecy and a bigger public profile. This was a task further complicated by the role popular culture plays in glamourising the SIS. The new security landscape also demanded that intelligence services across countries develop stronger alliances and sharing mechanisms.

4. Leadership should be firm and honest and, at the same time, modest. It is essential that people understand that the leader has integrity, and is fully committed to the success and optimal performance of the organisation, rather than personal promotion and gain. It is critical that a leader is surrounded by a capable leadership team that has an optimal balance of skills, experience and personalities. This leadership team cannot afford to suffer from groupthink. It must be honest with itself and encourage a free exchange of ideas and a willingness

to disagree in private, before consolidating and projecting a cohesive message outward.

5. Professionalism is integral to a leader. It is imperative to have detailed knowledge about how the organisation is structured and be able to demonstrate it. Personal involvement, understanding, and command of the organisation is key, as is the readiness to challenge conventional wisdoms, means and methods that have been established over time. This helps to guard against complacency and the unexpected.

6. Always be ready with an immediate response to crises. It is critical to always have a clear overall strategic direction and purpose for your organisation, and to be able to clearly convey this. A clear strategic direction is essential from the first day you take charge.

7. Accountability is at the core of good leadership. Responsibility can and often must be delegated, but ultimately a leader must be accountable and willing to shoulder the blame when things go awry. This helps build confidence and trust within a team. The essentials of good leadership tend to remain constant but the challenges that one faces, particularly in the field of security, change constantly.

8. While we do seem to be facing a period of uncertainty, it is worth noting that previous eras, the Cold War for

example, have also been marked by uncertainty. What marks this era as different is the speed at which change occurs, creating greater uncertainty.

Discussion

1. Issue: Key leadership lessons gained from the London attacks of 2005. There was a need to deal with the understandably extensive emotions that the attacks caused. It was critical to exert a measure of control over the situation to prevent the perception that such a terrible attack and tragedy was not being dealt with in the best possible way. This was necessary to prevent a drastic dip in morale and self-confidence both within government and wider society. There was also urgent need to provide the political leadership with very quick and good analysis. This was only possible due to the presence of capable intelligence.

2. Issue: Dealing with the issue of the lone actor terrorist, and steps that can be taken to deal with this threat with regard to both the intelligence service and on a societal level. Studies and analysis have shown quite convincingly that a majority of the terror attacks in Europe over the last five to six years have come from individuals who are not part of terror organisations. They are generally motivated by personal factors and may

occasionally be ideologically inspired from extremist groups. They very often have criminal records and tend to suffer from mental health problems, personality issues, and serious social frustrations. In order to deal with this effectively, there needs to be a stronger understanding of these causal issues, particularly in the education sector. This would empower society to be able to spot worrying signs and trends within individuals at risk. The situation is further complicated by how emotions today tend to get expressed through social media, although this does offer a starting point. We also need to find a balance by being alert to the right things.

3. Issue: Balancing the need for an open door and engagement, with the need for secrecy and a restriction of information in the security services. The balance lies in being able to discern between information that needs to be protected and information that can be shared. This is important because sharing information also helps to build trust. Maintaining secrecy works best when we solely focus on information that must be protected.

4. Issue: Whether there is a greater role for intelligence services to conduct discreet and informal diplomacy in an age of big power politics and increasingly frayed relations between Great Powers. Intelligence services do indeed have an

important role to play through discreet and informal diplomacy. At a time of fraught international relations, it is integral that lines of communication are kept open in all channels and sectors. The instinct to cut off communications during a period of difficult relations is often counter-productive and must be resisted. While diplomacy through secret channels is necessary, it is not sufficient and dialogue must take place at as many levels as possible, especially in times of great contention.

Country Presentations

Singapore, Australia, Brunei, Cambodia, Chile, Denmark, India, Indonesia, Jordan, Malaysia

- 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. For instance, ISIS constitutes the biggest national security threat for Malaysia. Far-right extremism was also identified as a concern for Australia, with fears that far-right extremism could spark reciprocal attacks in the country.

- In terms of country-specific threats, drug trafficking was identified as a major cause of concern for Cambodia. For Jordan, inflammation of sectarian tension and violence spilling over from neighbouring countries was regarded as a major threat. Countries such as Denmark also viewed cyber threats (e.g. cyber-attacks on government infrastructure) as a pressing issue of concern.

- Several of the countries made the point that national security is a complex issue and have sought to define their conception of security accordingly. Denmark stated that there is no one definition of national security, and has paid attention to the dynamic nature of the threat it faces. For example, Indonesia sees its national security threats as military, non-military, as

well as hybrid in nature. Further, the threat of influence operations and electoral interference was identified as a key national security threat. Indonesia, for instance, recently took steps to mitigate the threat of disinformation operations ahead of the recent Indonesian elections in April 2019. Other countries such as Cambodia highlighted the potential of social media platforms to amplify misinformation online.

- Solutions to overcome various national security threats were presented. Australia and Chile recommended better intelligence gathering as well as enhancing policing powers to enhance national security protection. Chile has emphasised that actions towards the ownership and control of firearms will also be undertaken. An online national registry for firearm ownership, for example, will be implemented. Increased requirements for the acquisition of weapons will be introduced. New obligations for firearms holders such as being subjected to a mental evaluation system will also be introduced. Brunei also alluded to strengthening community resilience between various multi-religious and ethnic groups within countries. Singapore discussed the SG Secure movement that aims to ensure citizens are prepared and can respond appropriately to national security threats.

Republic of Korea, Turkey, Myanmar, New Zealand, Norway, Philippines, Lao PDR, Sri Lanka

- Terrorism and ideological radicalisation were identified as major threats to the countries mentioned above. This included potential terrorist attacks on strategic locations within the countries, and the problems brought about by returning foreign fighters. Sri Lanka was also concerned over the resurgence of terrorist insurgency, while the Philippines and Myanmar both continue to face threats from insurgent fighters within their respective countries.
- Turkey pointed out slightly different concerns in relation to the IS in its country. While the IS is seen as a direct terror threat by other countries, in Turkey the biggest terror threat is that of the Partiya Karkerên Kurdistanê (PKK)/ Kurdistan Communities Union (KCK), which was responsible for about 2000 deaths. The PKK/KCK activities, though, are impacted by the IS. As the IS increased its activities in Syria, the PKK/KCK has sought to establish control the Syrian areas it called "cantons" through terror and oppression.

- Socio-economic risks were also identified as national security concerns. Lao PDR, for instance, viewed stagnating economic development as a risk which could threaten the fabric of social cohesion and unity. Similarly, the Republic of Korea identified rising socio-

economic issues such as inequality which could disrupt the social unity of citizens.

- Military tensions were also a cause for concern. The Republic of Korea, for instance, identified military tensions with North Korea and the proliferation of nuclear weapons as a potential flash point for conflict.

- While many countries highlighted cybercrime and terrorism as two of the main national security concerns, some countries specified other issues as sources of concern. For example, New Zealand is most concerned with the impact from natural disasters and calamities, while Norway is concerned over the effects of climate change and the impact of irregular migration could entail.

Sweden, Switzerland, Thailand, Italy, United States of America, Vietnam

- Risks of cyber-attacks were a commonly identified national security threat for the countries above. The issue of critical infrastructure protection was of particular concern for all countries.

- The threat of rising militarisation was also identified as a pressing concern. Sweden, for instance, identified the militarisation in the Baltic region and the risk of territorial annexation as a national security

threat. Influence operations, cyber disruptions and disinformation campaigns was identified as a major threat to national security by countries such as Sweden and the United States.

- Thailand identified potential political unrest as a national security concern. Terrorist insurgency in the country's restive south was also of concern, while illegal immigration by sea was of concern to Italy.

- Solutions to overcome the various concerns were presented. Sweden's total defence concept to build societal resilience against influence campaigns was highlighted. The United States' Infraguard program – a partnership between the FBI and members of the private sector – provides training for government officials and private citizens in the protection of critical infrastructure and capacity building exercises. Switzerland is rethinking its old stance of neutrality, as neutrality might not be as effective against evolving threats. Enhanced collaboration, capacity building and intelligence sharing were identified by Italy and Vietnam as crucial for tackling threats to national security.

Day-to-Day Programme

Monday, 8th April 2019

0630–0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0845hrs **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

0920hrs **All guests to be seated**

0920hrs **Arrival of Guest-of-Honour**

0930–0935hrs **Welcome Remarks**

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

0935–0950hrs **Opening Address**

Dr Vivian Balakrishnan
Minister for Foreign Affairs
Singapore

0950–1000hrs **Reception / Coffee Break**

0950–1005hrs **Group Photo-taking (Parallel Activity)**

0845hrs **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

1005–1100hrs **Reception / Coffee Break**

1100–1110hrs

Introduction to RSIS, CENS and APPSNO

Venue : MMB, Level 1, MMS

Speaker : **Shashi Jayakumar**
Senior Fellow, Head,
CENS,
RSIS, NTU, Singapore

1110–1210hrs

Session 1 : Drivers of Disruption

Venue : MMB, Level 1, MMS

Chairperson : **Shashi Jayakumar**
Senior Fellow, Head,
CENS,
RSIS, NTU, Singapore

Speakers : **Sabine Selchow**
Research Fellow
ARC-Laureate Program in International History
The University of Sydney
Australia
Nick Bisley
Head

School of Humanities and Social Sciences
Professor of International Relations
La Trobe University, Australia

Sean Gourley
Founder and CEO
Primer
United States of America

1210–1300hrs **Lunch**

1300–1415hrs **Syndicate Discussions**

Venue : Blue Group @ Capricorn Ballroom
Green Group @ Aquarius Ballroom
Yellow Group @ Pisces Ballroom

1415–1830hrs **Perspectivity Challenge**

Venue : Pool Garden, Pavilion, Level 5, MMS

1900–2100hrs **Networking Dinner**

Venue : AquaMarine, Level 4, MMS

❖❖❖

Tuesday, 9th April 2019

0630–0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0900–1000hrs **Session 2 : Disrupting Violent Extremism**

Venue : MMB, Level 1, MMS

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

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

Speakers : **Lorenzo Vidino**
Director
Program on Extremism

George Washington University
United States of America

Paul Jackson
Senior Lecturer in History
Faculty of Education and Humanities
University of Northampton
United Kingdom

Rohan Gunaratna
Professor of Security Studies
S. Rajaratnam School of International Studies
Nanyang Technology University
Singapore

1000–1015hrs **Coffee Break**

1015–1130hrs **Syndicate Discussions**

Venue : Blue Group @ Capricorn Ballroom
Green Group @ Aquarius Ballroom

Yellow Group @ Pisces Ballroom

1130–1330hrs **Lunch Lecture**

Venue : MMB, Level 1, MMS

Chairperson : **Shashi Jayakumar**
Senior Fellow, Head, CENS, RSIS, NTU, Singapore

Speaker : **Joseph Liow**
Dean, College of Humanities, Arts and Social Science
Tan Kah Kee Chair of Comparative and International Politics
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

1400hrs **Assemble at Hotel Lobby for Singapore Bicentennial Tour**

1415–1715hrs **Singapore Bicentennial Tour**

1730hrs **FREE and EASY (Networking Time)**
** Dinner is not provided*

❖❖❖

Wednesday, 10th April 2019

0630–0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0900–1000hrs **Session 3 : Cybersecurity and Disruption**

Venue : MMB, Level 1, MMS

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

Chairperson : **Benjamin Ang**
Senior Fellow, CENS, RSIS, NTU,
Singapore

Speakers : **Andrew Grotto**
William J. Perry International Security Fellow
Center for International Security and Cooperation
Research Fellow, Hoover Institution
Stanford University

United States of America

Danit Gal
Project Assistant Professor
Cyber Civilizations Research Center
Keio University Global Research Institute
Japan

Gwenda Fong
Director (Strategy)
CyberSecurity Agency
Singapore

1000–1015hrs **Coffee Break**

1015–1130hrs **Syndicate Discussions**

Venue : Blue Group @ Capricorn Ballroom
Green Group @ Aquarius Ballroom
Yellow Group @ Pisces Ballroom

1130–1400hrs **Lunch Discussion**

Venue : Vanda Ballroom, Level 5, MMS

Chairperson : **Teo Yi-Ling**

Senior Fellow, CENS, RSIS, NTU,
Singapore

Speakers : **Shashi Jayakumar**
Senior Fellow
Head, Centre of Excellence for National Security
Executive Coordinator, Future Issues and Technology
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Norman Vasu
Senior Fellow
Deputy Head, Centre of Excellence for National Security
Coordinator, Social Resilience Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

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

1400–1645hrs **FREE and EASY (Networking Time)**

1645hrs **Assemble at Hotel Lobby for Distinguished Dinner Lecture**

1730–1830hrs **Distinguished Dinner Lecture: Strategic Leadership: Managing Disruption for National Security**

Venue : Leo 1 to 3, Resorts World Convention Centre, Level 1 Resorts World Sentosa

Chairperson : **Shashi Jayakumar**
Senior Fellow, Head, CENS, RSIS, NTU, Singapore

Speaker : **Sir John Scarlett KCMG OBE**

1845–1915hrs **Cocktail Reception**

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

1930–2100hrs **Dinner**

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

2100hrs **Transportation to Marina Mandarin Singapore**

❖❖❖

Thursday, 11th April 2019

0630–0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0900–1100hrs **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 : **Gulizar Haciyakupoglu**
Research Fellow, CENS, RSIS, NTU, Singapore

Presenters : By alphabetical order starting with host country: ***Singapore, Australia, Brunei Darussalam, Cambodia, Chile, Denmark, India, Indonesia, Republic of Korea, Jordan, Turkey, Malaysia***

1100–1115hrs **Coffee Break**

1115–1215hrs **Session 4 : Technology and Society**

Chairperson: : **Teo Yi-Ling**
Senior Fellow, CENS, RSIS, NTU, Singapore

Speakers : **Jack Linchuan Qiu**
Professor
School of Journalism and Communication
Chinese University of Hong Kong
Hong Kong

Shihoko Goto
Deputy Director for Geoeconomics
Senior Associate for Northeast Asia, Asia Program
Wilson Center
United States of America

Sabrina Luk Ching Yuen
Assistant Professor
Public Policy and Global Affairs
School of Social Sciences
Nanyang Technological University
Singapore

1215–1300hrs **Lunch**

1300–1415hrs **Syndicate Discussions**

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

1415 – 1530hrs **FREE and EASY (Networking Time)**

1530hrs **Assemble at Hotel Lobby for Visit to Cybersecurity Institute**

1600 – 1800hrs **Visit to Cybersecurity Institute**

1830hrs **FREE and EASY (Networking Time)**

❖❖❖

Friday, 12th April 2019

0630–0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0900–1000hrs **Session 5 : Case Studies**

Venue : MMB, Level 1, MMS

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

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

Speakers : **Angel Hsu**
Assistant Professor

Social Sciences (Environmental Studies)
Yale-NUS
Singapore

Jennifer Daskal
Associate Professor of Law
American University
Washington College of Law
United States of America

Olli Kangas
PhD, Program Director
The Strategic Research Council at the Academy of Finland
Professor of Practice, Department of Social Research
University of Turku
Finland

1000–1110hrs

Syndicate Discussions

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

Coffee Break

1115–1315hrs **Country Presentation on Homeland Security Management**

Venue : MMB, Level 1, MMS

Chairperson : **Gulizar Haciyakupoglu**
Research Fellow, CENS, RSIS, NTU, Singapore

Presenters : By alphabetical order:
Myanmar, New Zealand, Norway, Philippines, Lao PDR, Sri Lanka, Sweden Switzerland, Thailand, Italy, United States of America, Vietnam

1315–1415hrs **Lunch**

1415–1830hrs **FREE and EASY (Networking Time)**

1830–1900hrs **Cocktail Reception**

1900–1945hrs **13th APPSNO Certificate Presentation Ceremony**

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

1945 – 2130hrs **Closing Dinner**

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

❖❖❖

List of Guest-of-Honour and Speakers

GUEST-OF-HONOUR	**Dr Vivian Balakrishnan** Minister for Foreign Affairs Singapore
SPEAKERS	**Benjamin Ang** Senior Fellow; Coordinator Cyber and Homeland Defence Programme Centre of Excellence for National Security S. Rajaratnam School of International Studies Nanyang Technological University, Singapore
	Nick Bisley Head School of Humanities and Social Sciences Professor of International Relations La Trobe University Australia
	Jennifer Daskal Associate Professor of Law American University

Washington College of Law
United States of America

Gwenda Fong
Director (Strategy)
CyberSecurity Agency
Singapore

Danit Gal
Project Assistant Professor
Cyber Civilizations Research Center
Keio University Global Research Institute
Japan

Shihoko Goto
Deputy Director for Geoeconomics
Senior Associate for Northeast Asia, Asia Program
Wilson Center
United States of America

Sean Gourley
Founder and CEO
Primer
United States of America

Andrew Grotto
William J. Perry International Security Fellow

Center for International Security and Cooperation
Research Fellow, Hoover Institution
Stanford University
United States of America

Rohan Gunaratna
Professor of Security Studies
S. Rajaratnam School of International Studies
Nanyang Technology University
Singapore

Angel Hsu
Assistant Professor
Social Sciences (Environmental Studies)
Yale-NUS
Singapore

Paul Jackson
Senior Lecturer in History
Faculty of Education and Humanities
University of Northampton
United Kingdom

Shashi Jayakumar
Senior Fellow
Head, Centre of Excellence for National Security

Executive Coordinator, Future Issues and Technology
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

Olli Kangas
PhD, Program Director
The Strategic Research Council at the Academy of Finland
Professor of Practice, Department of Social Research
University of Turku
Finland

Joseph Liow
Dean, College of Humanities, Arts and Social Science
Tan Kah Kee Chair of Comparative and International Politics
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

Sabrina Luk Ching
Assistant Professor
Public Policy and Global Affairs

School of Social Sciences
Nanyang Technological University, Singapore

Jack Linchuan Qiu
Professor
School of Journalism and Communication
Chinese University of Hong Kong
Hong Kong

Sir John Scarlett KCMG OBE
Former Chief of the British Secret Intelligence Service

Sabine Selchow
Research Fellow
ARC-Laureate Program in International History
The University of Sydney
Australia

List of Chairpersons

CHAIRPERSONS

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

Gulizar Haciyakupoglu
Research Fellow
Cyber and Homeland Defence Programme
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Shashi Jayakumar
Senior Fellow
Head, Centre of Excellence for National Security
Executive Coordinator, Future Issues and Technology
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

Yi-Ling Teo
Senior Fellow
Cyber and Homeland Defence Programme
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Norman Vasu
Senior Fellow
Deputy Head, Centre of Excellence for National Security
Coordinator, Social Resilience Programme
S. Rajaratnam School of International Studies
Nanyang Technological University, Singapore

List of Participants

AUSTRALIA	**Michael Burke** Assistant Secretary Transnational Crime Policy Branch Department of Home Affairs Australia
BRUNEI DARUSSALAM	**Hajah Halipah Kamaluddin** Assistant Director Strategic Operations Brunei Research Department Prime Minister's Office Brunei Darussalam
CAMBODIA	**Yuth, Sophanarith** Brigadier General Deputy Director External Operations Department General Department of Research and Intelligence Cambodia
CHILE	**Patricio Aguirre** Counsellor Deputy Director International and Human Security Ministry of Foreign Affairs Chile

DENMARK	**Morten Sørensen** Senior Adviser Danish Security and Intelligence Denmark
INDIA	**Kanchan Lakshman** Joint Director National Security Council Secretariat India
INDONESIA	**Erwin Herviana Suherman** Senior Agent State Intelligence Agency (BIN) Indonesia
INDONESIA	**Andy M Taufik** Air First Marshal Coordinating Ministry Political, Legal, and Security Affairs of the Republic of Indonesia Assistant Deputy Defence Intelligence Coordination Indonesia

ITALY	**Luca Vincenzo Maria Salamone** Deputy Director Innovation and Technology Directorate Secretariat General of Defence and National Armaments Directorate Ministry of Defence Italy
JORDAN	**Mohammad Al Rahahleh** Assistant Regional Commander Jordan Police Directorate Jordan
LAO PDR	**Khanthaly Phommacahan** Lieutenant-Colonel Acting Chief of Bureau Intelligence Department Ministry of Public Security Lao People's Democratic Republic
LAO PDR	**Khaophone Phommachanh** Head of Information Division Interpol Department General Department of Police Ministry of Public Security Lao People's Democratic Republic

MALAYSIA	**Mohammad Azri Bin Mohtar** Deputy Director Prime Minister's Department Malaysia
MYANMAR	**San Ko** Police Colonel Head of International Department Special Branch Myanmar Police Force Myanmar
NEW ZEALAND	**Kim Beaumont** Senior Advisor National Security Systems Directorate Department of the Prime Minister and Cabinet New Zealand
NORWAY	**Harald Fardal** Chief Analyst Norwegian Directorate Civil Protection Norway
PHILIPPINES	**Roberton G. Lapuz** Chief Directorial Staff National Intelligence Coordinating Agency Philippines

REPUBLIC OF KOREA	**Kim Joon** Deputy Director Cooperation and Coordination Division National Counter Terrorism Center Republic of Korea
REPUBLIC OF KOREA	**Park Sun Gil** Director of Cooperation and Coordination Division National Counter Terrorism Center Republic of Korea
SINGAPORE	**Ang Choon Kiat (Hong JunJie)** Deputy Director Emergency & Contingency Planning Division Public Transport Group Land Transport Authority Ministry of Transport Singapore
SINGAPORE	**Chew Lip Ping** Director (Cybersecurity) Government Security Group Government Technology Agency Prime Minister's Office Singapore

SINGAPORE

Chew Ming Chiang
Vice President
General Manager
Kinetics Integrated Services
ST Engineering Land Systems Ltd
Singapore

SINGAPORE

Chin Siew Fei
Deputy Director-General
International Economics Directorate
Ministry of Foreign Affairs
Singapore

SINGAPORE

Choo Lee See
Divisional Director
Infrastructure & Facility Services Division
Ministry of Education
Singapore

SINGAPORE

Fong Peng Keong
Director
Pollution Control Department
National Environment Agency
Ministry of the Environment and Water Resources
Singapore

SINGAPORE

Foo Li Yen
Deputy Commander (Compliance)
Integrated Checkpoints Command (Air)
Immigration & Checkpoints Authority
Ministry of Home Affairs
Singapore

SINGAPORE

Gay Teck Chuan Gavin
Assistant Director Operations
Specialist Capabilities & Doctrines Division
Operations Department
Singapore Police Force
Ministry Of Home Affairs
Singapore

SINGAPORE

Goh Chew Hwee, Karen
Deputy Commander (Domain Security)
Integrated Checkpoints Command (Land)
Immigration & Checkpoints Authority
Ministry Of Home Affairs
Singapore

SINGAPORE

Goh Hoon Lip
Head
Policy and Research
Policy & Planning Division
Singapore Customs
Ministry of Finance
Singapore

SINGAPORE

Eugene Goh Wei Lieang
Commanding Officer
Singapore Prison Emergency Action Response Force
Singapore Prison Service
Ministry of Home Affairs
Singapore

SINGAPORE

Heng Chun Howe Vincent
Acting Director
(Organisational Resilience)
Corporate Development Group
Housing & Development Board
Ministry of National Development
Singapore

SINGAPORE

Huang Meiyu Audris
Head
Human Resource Management
Corporate Development
Ministry of Finance
Singapore

SINGAPORE **Lee Hwee San**
Deputy Director Supply Chain Management
Resource_Management Division Operations Group
Ministry of Health
Singapore

SINGAPORE **Jasminder Singh s/o Bilveer Singh**
Senior Analyst
International Centre for Political Violence and Terrorism Research
S. Rajaratnam School of International Studies (RSIS)
Singapore

SINGAPORE **Jesse Lee Wee Yap**
Deputy Director
Intelligence Department
Foreign Manpower Management Division
Ministry of Manpower
Singapore

SINGAPORE **Lim Han Kiong**
Director (Operations)
Defence Cyber Organisation
Ministry of Defence
Singapore

SINGAPORE **Lim Poh Chuan**
Branch Head
2nd People's Defence Force
Island Defence Task Force
Singapore Armed Forces
Ministry of Defence
Singapore

SINGAPORE **Lim Thian Chin**
Deputy Director
Critical Information Infrastructure
CyberSecurity Agency of Singapore
Ministry of Communications and Information
Singapore

SINGAPORE **Lim Yong Seng Vincent**
Director (Investigations)
Investigations Department
Corrupt Practices Investigation Bureau
Prime Minister's Office
Singapore

SINGAPORE **Lin Zhenxing**
Deputy Superintendent (Auxiliary Police Force)
Head Development
Certis CISCO Auxiliary Police Force Pte Ltd
Certis CISCO Security Pte Ltd
Singapore

SINGAPORE **Ng Thiam Poh Daniel**
Director
Information Exploitation
Information Division
DSO National Laboratories
Singapore

SINGAPORE **Ong Chor Kiat, Colin**
Deputy Director
Gas Industry Regulation Department
Ministry of Trade and Industry
Singapore

SINGAPORE **Oon Chin Yong Jeffrey**
Deputy Director
Corporate & Infocomms Security Audit
Ops Tech Group
Ministry Of Home Affairs
Singapore

SINGAPORE **Poon Ngee**
Deputy Director
Home Team Simulation System
Centre for Home Team Skills Transformation
Home Team Academy
Ministry of Home Affairs
Singapore

SINGAPORE

Sim Yuze Gabriel
Deputy Head (Water System Unit)
Joint Operations Department
Public Utilities Board
Ministry of Environment & Water Resources
Singapore

SINGAPORE

Tan Choon Meng
Branch Head
Military Security Department
Ministry of Defence
Singapore

SINGAPORE

Tan Nan An, Harris
Branch Head
Joint Intelligence Department
Singapore Armed Forces
Ministry of Defence
Singapore

SINGAPORE

Tan Peng Peng, Amanda
Acting Director
International Engagements Directorate
International Cooperation & Partnerships Division
Ministry of Home Affairs
Singapore

SINGAPORE

Tan Puay Seng
Deputy Director
Corporate Relations and Engagement
Centre for Planning, Communications and Engagement
Home Team Academy
Ministry of Home Affairs
Singapore

SINGAPORE

Tan Zhi Xiang, Kelvin
Deputy Director (Policy & Analytics)
National Security Coordination Centre
National Security Coordination Secretariat
Prime Minister's Office
Singapore

SINGAPORE

Tay Choong Hern
Ops Manager
182 Squadron, Maritime Security Task Force
Republic of Singapore Navy
Ministry of Defence
Singapore

SINGAPORE

<u>Teo</u> Wee Meng
Assistant Director
Technology Crime Division
Criminal Investigation Department
Singapore Police Force
Ministry of Home Affairs
Singapore

SINGAPORE

<u>Teo</u> Wee Teck
Assistant Director
Police Intelligence Department
Singapore Police Force
Ministry of Home Affairs
Singapore

SINGAPORE

<u>Tham</u> Borg Tsien
Deputy Director
ASEAN Directorate
Ministry of Foreign Affairs
Singapore

SINGAPORE

<u>Yeo</u> Tiong Yeow
Director
Resilience & Preparedness Division
Info-Communications Media Development Authority
Singapore

SRI LANKA	**Senarath Wijesooriya** Director Naval Welfare Naval Headquarters Sri Lanka Navy Sri Lanka
SWEDEN	**Fredrik Konnander** Head Counter Influence Branch Swedish Civil Contingencies Agency Sweden
SWITZERLAND	**Philipp Kronig** Head of Information Management/Cyber Federal Intelligence Service Switzerland
THAILAND	**Thammarat Rattanamanee** Director of Secretariat of Intelligence Advisory Board National Intelligence Agency Thailand
TURKEY	**Burhan Bahadir İÇMEGİZ** 2nd Degree Chief Superintendent Deputy Head of International Relations Department Turkish National Police Turkey

TURKEY	**Ozlem Akpinar Cam** Chief of Division Turkish Presidency Turkey
UNITED STATES OF AMERICA	**Sharon Kuo** Legal Attaché Federal Bureau of Investigation (FBI) United States of America
VIETNAM	**Minh Hieu Nguyen** Director General Foreign Relations Department Ministry of Public Security Vietnam

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.
For more information about CENS, please visit www.rsis.edu.sg/research/cens/.

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

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.