**Event Report**

# Asia-Pacific Programme for Senior National Security Officers: Boundaries of National Security

**6-11 May 2018**

**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**:
Muhammad Faizal bin Abdul Rahman, Juhi Ahuja, Nur Diyanah binte Anwar, Joseph Franco, Cameron Sumpter, Dymples Leong Suying, Pravin Prakash, Romain Brian Quivooij and Jennifer Yang Hui
**Editors**:
Cameron Sumpter
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.

# Contents

# EXECUTIVE SUMMARY

The 12th annual Asia-Pacific Programme for Senior National Security Officers (APPSNO) was held at Marina Mandarin Singapore from 6-11 May 2018. 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 the "Boundaries of National Security".

Speakers from a range of nations, including the United States, Japan, Turkey, Australia, the United Kingdom, Israel, Sweden, Latvia, and Singapore shared their expertise and experiences on the following topics:

1. **Emergent Issues in Homeland Security** – drones, predictive policing, strategic disinformation campaigns and biotechnology

2. **Governing Difference** – rising inequality, multicultural societies, race relations, migration and social cohesion

3. **Terrorism and its Futures** – reciprocal radicalisation, the rise of violent far-right organisations and the direction of jihadi movements in Southeast Asia

4. **Cybersecurity: Boundaries and Securities** – human resource challenges, critical infrastructure protection and cybercrime

5. **Case Studies** – migrant inclusion in Sweden, resilience amid complex risks, and the current wave of populist politics

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-nine participants from 24 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 Manpower and Second Minister for Home Affairs Mrs Josephine Teo opened the programme by highlighting the broadening 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 Mr Michael Shoebridge from the Australian Strategic Policy Institute (ASPI), who outlined several major global trends based on recent history and the subsequent arrival of new priorities for international security.

# Presentation Summaries

## Session 1: Emergent Issues in Homeland Security

Not so Fast: Considerations for Adopting New Technologies in Policy
**Arthur Michel**, *Co-director, Centre for the Study of the Drone, Bard College, United States*

> Drones, social media monitoring, and predictive policing are three emerging technologies for safeguarding national security. Each development holds promise but all three come with associated challenges.

Information Warfare: Defending the Digital Engagement Space
**Donara Barojan**, *Assistant Director, Research and Development, Digital Forensic Research Lab, NATO Stratcom Centre of Excellence, Latvia*

> Social media platforms have led to echo chambers, rendering electorates susceptible to disinformation campaigns. The NATO lab flag broad disinformation campaigns by exposing tactics and narratives rather than simply debunking individual stories through algorithms and detection systems.

Biotechnology and National Security
**Piers Millett**, *Principal, Biosecure Ltd, United Kingdom*

> Advances in biotechnology present opportunities for the improvement of lives. However, the dual-use nature of the associated developments presents potential dangers. Enhanced oversight through partnerships and proper risk communication among the various stakeholders are essential.

Distillation

1. While new technologies may promise strategic and operational benefits for law enforcement, enthusiasm must be tempered by awareness of the shortcomings of certain innovations and their uses in the hands of adversaries.

2. The viral spread of disinformation has become an inexpensive and potent tool for manipulating populations and undermining key institutions in other nations. Establishing effective means of countering such strategies may be as vital as protecting national borders and critical infrastructure.

3. Advancements in biotechnology are creating opportunities to develop pathogens more affordably and in labs which are difficult to detect. Governments will need to establish crucial partnerships with the biotech sector to keep abreast of potential threats.

# Session 2: Governing Difference

The Corruption of Capitalism: Why Rentier Capitalism and the Growing Precariat Are Threats to Social Stability
**Guy Standing**, *Professorial Research Associate, School of Oriental and African Studies, University of London*

> The neoliberal economic model developed in the 1980s created a system of rentier capitalists, with the majority of income going to a small group. The resulting Precariat – a section of society which experience low wages and insecure work conditions – may be motivated to mobilise against capitalism, thereby creating social instability.

Governing Difference
**Tim Soutphomassane**, *Race Discrimination Commissioner, Australia*

> According to the OECD, Australia has one of the highest proportions of immigrants in the world. Cultural integration is therefore a key part of Australia's overall integration policy, while maintaining a secular national identity. Australia has also developed legal and non-legal means to combat racism within its society.

Scholarship and Urban Policies beyond Diversity
**Ayse Caglar**, *Professor, Department of Social and Cultural Anthropology, University of Vienna*

> With increasing numbers of migrants and refugees settling in cities, there is a need to govern differences between groups to ensure social cohesion, economic prosperity and security. More needs to be done to establish an analytical vocabulary to capture the relationship between migrants and cities in urban redevelopment.

Distillation

1. Local governments need to review the economic, political and historical conditions of contexts which have caused certain groups to lag behind others. Policies and strategies can be developed further to assist these groups.

2. Maintaining social stability is a priority for most societies as this ensures security and economic development. Authorities should therefore prioritise services and activities that encourage social cohesion.

3. There is value in comparative research on the effects of governance in multicultural societies, and identifying how strategies implemented in these societies can be adapted as best practice. Insight can also be attained by looking into the legal and non-legal means to govern differences, as well as grassroots efforts to encourage social cohesion.

# Session 3: Terrorism and its Futures

Radicalisation Spiralling Effects: The Interconnectedness of Different Forms of Extremism
**Julia Ebner**, *Research Fellow, Institute for Strategic Dialogue*

> Far right and Islamist extremist groups share a number of common features. Their communication strategies and recruitment drives bear remarkable similarities in form and content.

From Memes to Marches: How Boots-on-the-Ground Events in 2017 Fractured the US Radical Right
**Susy Buchanan**, *Editor, Intelligence Project, Southern Poverty Law Centre*

> Members of far-right groups have recently held rallies in US cities. The Southern Poverty Law Center (SPLC) pays close attention to the activities of these organisations and has developed a three-pronged action plan to reduce prejudices in schools, to take legal action against extremist groups and monitor the activities of extremist groups.

The Future of Terrorism in Southeast Asia: Some Preliminary Thoughts
**Kumar Ramakrishna**, *Associate Professor, Head of Policy Studies and Coordinator of the National Security Studies Programme, RSIS*

> Terrorism in Southeast Asia is likely to take different forms. Efforts to improve governance and fight Islamophobia are crucial in countering this multifaceted threat.

Distillation

1. Far-right and Islamist extremist groups may be two sides of the same coin. Similarities show that violent extremist networks are more connected than one might think.

2. While US far-right groups have gained prominence over the last year, their influence seems to be in a process of decline. It is too early to know whether this evolution will be a lasting trend, but it reveals rapid changes in the landscape of far-right extremism in the US.

3. Terrorism in Southeast Asia is an enduring phenomenon. Governments must establish effective combinations of “hard” and “soft” measures (such as police operations on the one hand, and counter-radicalisation programmes on the other), and work towards greater intra- and inter-state coordination and information sharing.

# Session 4: Cybersecurity: Boundaries and Securities

How Japan is Closing a Cybersecurity Gap Toward Tokyo 2020
**Mihoko Matsubura**, *Adjunct Fellow, Pacific Forum, Japan*

> The Japanese government aims to tackle the human resource challenge of shortages in cybersecurity talent. Specialised education and training initiatives for the next-generation of professionals will ensure a robust infrastructure to tackle the complexities of the cybersecurity landscape.

Cybersecurity Cosmos: Boundaries and Priorities
**Greg Austin**, *Professor, Australian Centre for Cyber Security, University of New South Wales (Canberra), Professional Fellow, EastWest Institute, Australia*

> Impending challenges in cyberspace revolve around three intractable problems: cybercrime, critical infrastructure protection and content control. The rapid advancement of emerging technologies adds new dimensions to national security threats in the future.

The Blurred Boundaries between Cybercrime and National Security
**Lior Tabansky**, *Head of Research Development, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv*

> Cybercrime as a Service (CaaS) will play a prominent role in the future of cybercrime as cooperation among criminal elements and hostile entities evolves over time. Internal security contractors or private corporations can market cyber services to both state and non-state actors.

Distillation

1. There is a global shortage in cybersecurity human resources. Nations throughout the world have taken steps to mitigate shortfalls by mentoring, training and educating next-generation experts through various initiatives and collaborating with cyber industry experts.

2. International cybersecurity cooperation is paramount. No country can deliver adequate protection of critical infrastructure in cyberspace on its own. Therefore, both regional and international collaboration should be reflected in national cybersecurity strategy.

3. The enhancement of diplomatic and inter-governmental collaboration should also account for cyber norms (especially where the boundaries of cyberspace are increasingly blurred) and share best practices to mitigate threats.

# Session 5: Case Studies

Immigration and Integration: Key Sources for Development
**Sofia Appelgren**, *Founder, Mitt Liv, Sweden*

> While Sweden's integration policies are deemed successful, access to its labour market remains a huge challenge for most immigrants. The lack of state focus on inclusion is met by a rise in social enterprises, such as Mitt Liv, which works toward instituting more inclusive practices in the workplace.

*Understanding and Managing the New Dimensions of Emerging Threats and Complex Risks*
**Rebecca Nadin**, Head, Risk and Resilience Programme, Overseas Development Institute, United Kingdom

> Building resilience requires a better understanding of multi-dimensional threats and risks. It also entails mapping threat ecosystems and intersections with other dangers to identify possible risk pathways and the most relevant entry points for intervention.

Populism and its Discontents
**John Judis**, *Author and Journalist, United States*

> Demographic change, including a hollowing out of the middle class and the emergence of metro-cities dominated by well-educated elites and a migrant working class have greatly impacted American politics. Populism is a warning signal of discontent.

Distillation

1. Resilient societies require a critical understanding of emerging threats and the multi-dimensional risks they may pose. They also necessitate a deeper level of engagement between all stakeholders.

2. While societies focus on the integration of migrants, governments must pay close attention to levels of inclusion and new arrivals' access to grassroots networks. Failing to do so may create a conundrum where immigrants are welcomed but fail to access the ties that bind society together, resulting in disconnectedness, isolation and eventually fractured communities.

3. Populism is predicated on the notion of an existing disconnect between elites and the rest of society. It comes to the fore in times of polarisation and its presence is a warning signal of intractable social problems.

# Lunch Discussion: Singapore's National Security Past, Present, and Future

Society and National Security
**Norman Vasu**, *Senior Fellow and Deputy Head, CENS*

> Singapore's national security narrative is largely constructed around the notion of vulnerability, which justifies strategies that protect sovereignty and public order. Singapore faces the challenge of sustaining the 'Garrison state' and altering the national security narrative to ensure societal resilience.

Terrorism and Radicalisation
**Shashi Jayakumar**, *Senior Fellow and Head, CENS*

> Circumstances surrounding radicalisation and terrorism have evolved significantly since the 2001 JI (Jemaah Islamiyah) arrests in Singapore. As the profiles of radicalised individuals become more complex, the state is faced with the challenge of devising new strategies for deradicalisation, rehabilitation and reintegration.

Cybersecurity and Technology
**Benjamin Ang**, *Senior Fellow and Coordinator of the Cyber and Homeland Defence Programme, CENS*

> Singapore recognises four key threats to its cyber security landscape: ransomware, defacement, phishing, and command and control servers (DDOS). The nation's broad strategy is to balance digital opportunities with digital risk.

Distillation

1. The manifestation of xenophobic and intolerant attitudes in Singapore highlights the importance of ensuring communal harmony as a basic tenet of national security.

2. Singapore places great emphasis on the 'bouncebackability' of the nation, as highlighted by the SGSecure initiative. Although Singapore's security establishment is reasonably successful in terms of counter-terrorism strategy, vulnerabilities remain due to social cleavages. Singapore needs to pay close attention to disinformation campaigns and learn from the experiences of affected countries.

3. Singapore recognises that as it embraces the rapid advancement of technology, threats to its cyber and digital landscape will become more complex. The nation must strike a balance between opportunities and risk.

4. Security discourse in Singapore is historically top-down. Policy makers need to ensure that "slow-burn" threats can be addressed by citizens organically and with a degree of independence.

# Distinguished Dinner Lecture

The Boundaries of National Security: Recent History, Global Trends and Emerging Priorities
**Michael Shoebridge**, *Director, Defence and Strategy, Australian Strategic Policy Institute, Australia*

> Trends that continue to shape the environment include population growth, demographic change, expansive urbanisation, mass people movement, climate change, an information explosion, technological development and the shift of economic gravity to Asia.

Distillation

1. Global trends are changing the national security environment. Law enforcement and security agencies must evaluate their strategic and operational assumptions and evolve to keep pace with rapid change.

2. Understanding trends is crucial to anticipating plausible security concerns of the future. While states have a key role in anticipating security concerns, the growing prominence of non-state actors will present ongoing challenges.

3. States must broaden international partnerships through multilateral platforms and pursue partnerships with non-state actors such as universities and technology companies.

# Opening Address

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

Ambassador Ong Keng Yong opened the 12th Asia-Pacific Programme for Senior National Security Officers (APPSNO) by highlighting the significance of the programme's theme, "Boundaries of National Security". Security threats now derive from a range of sources, including home-grown terrorism, natural disasters, economic decline and social unrest. States need to develop the ability to identify which domain(s) different issues fall under, react effectively to the changing contexts surrounding these issues, and deal with threats through coordinated strategies.

# Ministerial Address

**Mrs Josephine Teo**
*Minister for Manpower and Second Minister for Home Affairs, Singapore*

1. The definition of national security has evolved, from a traditional focus on military and homeland security, to one involving broader dimensions such as economic and energy concerns. Social issues now have important implications for security; for example, disagreements developed online can spill over to violence in the physical world. The three key national security concerns in Singapore today are terrorism, cybersecurity, and deliberate online falsehoods.

2. First, Singapore is not immune to the threat of violent extremism. Terrorist organisations have declared Singapore a target, and the number of 'self-radicalised' individuals detained in Singapore has increased sharply over the last two years. Responding to the evolving challenge, Singapore has enhanced laws to strengthen infrastructure protection and event security. The Singapore Police Force has introduced new Emergency Response Teams and In-Situ Reaction Teams capable of responding swiftly following an attack. The government has also launched its SGSecure strategy, a national movement to enhance community vigilance, preparedness and unity.

3. Second, the two principal threats in cyberspace are cyberattacks and self-radicalisation through online content. To counter cyberattacks, Singapore recently formed the Cyber Security Agency (CSA) and passed the Cybersecurity Bill to strengthen the protection of computer systems. Singapore is also partnering with private companies and industry experts worldwide to counter cyberattacks and develop expertise. Online self-radicalisation through extremist propaganda has also become an issue in Singapore. The government has called on family, colleagues and friends to be the first line of defence in identifying troubling behaviour and alerting authorities.

4. Third, deliberate online falsehoods spread quickly and gain traction in the physical world. Fake news stories have exploited racial and religious fault-lines and have the power to erode societal trust. In this regard, the Singapore Parliament established a Select Committee on Deliberate Online Falsehoods to hear testimonies from social

media companies, specialists and academics on the repercussions of online falsehoods.

5. Engagement and strategic collaboration is essential. Both civil society and the business community have roles to play in safeguarding Singapore against these threats. Challenges to national security are increasingly complex and interdependent.

## Session 1: Emergent Issues in Homeland Security

### Not so Fast: Considerations for Adopting New Technologies in Policy

**Arthur Michel**, *Co-director, Centre for the Study of the Drone, Bard College, United States*

1. Law enforcement agencies now use drones for surveillance and situational monitoring as they are relatively inexpensive, quick to deploy, easy to use and have a wide range of applications. However, limitations include their inability to fly for long durations, operate at high altitudes or at night, and the often low resolution of their sensors.

2. Developers have experimented with a number of methods to counter the use of drone technology but no solution has proven absolutely effective. Drones may be detected by radar, but can be confused for birds. Electro-optical detection has similar identification issues and cannot see beyond the line of sight. Acoustic recognition is another strategy; libraries of drone sounds have been created, but if a particular drone is not listed, the system will be effectively deaf. The same is true for Radio-Frequency (RF) sensor libraries.

3. Drones may be taken down by signal jamming, though this is disruptive and illegal in many countries. Nets can be deployed to capture drones but accuracy is difficult and free-falling drones may be dangerous. Spoofing is a cyber-method which attempts to control a drone by replicating its control signals, but this approach is open to counter hacking. Lasers raise safety concerns as electromagnetic pulses can damage voltage surges in the surrounding area, while water cannons simply do not work very well. An additional challenge is the current reality of swarms of integrated drones, which can disrupt law enforcement operational awareness and currently have no effective counter-measure.

4. Social media monitoring can track online behaviour such as potential radicalisation and cybercrime planning. However, governments may use the same technology to curtail dissent. Online behavioural prediction combined with social network analysis can be a powerful tool for identifying threats but it may also create a chilling effect and undermine privacy.

5. Predictive policing uses software to identify individuals (either victims or perpetrators) and the geographical data of where a crime might occur based on historical information. However, a lack of statistical data means there is insufficient evidence to show whether predictive policing effectively prevents crime.

## Information Warfare: Defending the Digital Engagement Space

**Donara Barojan**, *Assistant Director, Research and Development, Digital Forensic Research Lab, NATO Stratcom Centre of Excellence, Latvia*

1. The onset of social media and the decentralisation of information dissemination has magnified the effectiveness of disinformation campaigns that currently threaten democracies throughout the world. Social media, which is an immense, fast-moving and under-regulated space, lowers entry barriers to the information environment for both state and non-state actors. These factors make disinformation a high-impact-low-cost means of exploitation or attack.

2. The vulnerabilities of social networks are embedded within their functional design. When users read a story on Facebook they often attribute the trust they have for the person posting the article to the content itself. Algorithms provide suggestions for media based on a user's preferences, creating echo chambers in which the user is not exposed to opposing views. While in the past a media consumer would have to actively avoid contending views to find herself in an echo chamber, today users must actively seek different opinions to break free from social media echo chambers created by default.

3. NATO's Digital Forensic Research Lab uses open source and digital forensic research to analyse the spread of disinformation on social networks. The lab exposes tactics and narratives used to spread disinformation and follows manipulative campaigns in real time throughout the world to protect the integrity of elections.

4. One of the lab's key intentions is to ensure social media monitoring and network analysis is used to flag broad disinformation campaigns by exposing tactics and narratives rather than simply debunking individual stories. The lab strives to update and improve its algorithms and detection systems to keep pace with those who misappropriate social media platforms with malicious intent.

5. The NATO lab has conceptualised 'four Ds' of disinformation tactics used by the Russian government: (1) Dismiss the critic; (2) Distort the fact; (3) Distract from the main issue; and (4) Dismay the audience. Each tactic was witnessed in Moscow's counter reactions following the annexation of Crimea, the shooting down of Malaysian Airlines flight MH17, and the recent Skripal poisoning in the UK. As a basic analytical framework, the four Ds explain the threat of disinformation to media consumers and develop safeguards.

6. Another framework is the use of eight common logical fallacies which spread disinformation. For example, ad hominem attacks on journalists; appealing to the emotions of readers/listeners; and accusations of hypocrisy. Explanations through the prism of logical fallacies expand thinking of the issue beyond simply 'fake news' by highlighting that hostile narratives can also be reinforced by minor inaccuracies and common biases. Since a hostile entity can target a whole region, it is important to monitor domestic information spaces and seek regional cooperation.

## Biotechnology and National Security

**Piers Millett**, *Principal, Biosecure Ltd, United Kingdom*

1. Biotechnology is changing how we create things, how we feed ourselves and how we stay healthy. As a powerful dual-use technology, its impact is dependent on the intent of the user. Traditional national security threats include the potential production of bioweapons, while non-traditional risks include health, production, and energy security

concerns. Given the considerable complexity, governments will need to develop and maintain effective relationships with the biotech sector as technology matures.

2. Over the past five to ten years, almost all of the technical barriers to making biological weapons have eroded, though these capabilities are still more likely to be in the hands of states than non-state actors. One contemporary issue that should alarm national security advisors is the increasing difficulty of detection. In the past, production facilities involved significant metal infrastructure in fixed identifiable positions. Today the biotech industry is more about flexible manufacturing. Plastic is used instead of metal, which makes it much easier to shift from one activity to another much more quickly.

3. The juncture of cyber security and biotechnology presents an important risk, particularly regarding unauthorised access to data, information or knowledge and the ability to secretly alter that data, information or knowledge. Traditional biosecurity was concerned with locking up 'bugs'. The emergence of the cyber dynamic illustrates how quickly priorities are changing.

4. Almost every nation in the world approaches biosecurity through control lists, which comprise archives of biological agents and outline the regulation of licenses and establishment oversights required to work with such dangerous materials. However, as the lists categorise agents by name and not their specific biological make-up, they can fail to capture the whole range of concerning biological agents while including others that may not be harmful.

5. When assessing the threat of a biological agent, the two key issues are whether it can be transformed into a harmful toxin and manufactured in the form of spores to facilitate dissemination. Enhanced oversight through partnerships, ongoing relationships and effective risk communication among various stakeholders are essential to prepare for potential biological attacks.

## Syndicate Discussion

1. *Emerging technologies may be misused.* Drones have been hijacked through various non-kinetic means such as spoofing or jamming. Legitimate biotechnology research might have dual uses which can be exploited for nefarious purposes such as industrial sabotage or the manipulation of laboratory data. The misuse of new technology can also affect security operations. For example, a criminal gang unleashed a swarm of drones to disrupt and obscure the view of FBI agents conducting a hostage rescue mission in late 2017. Bomb-laden drones also attacked two Russian military bases in Syria in January 2018.

2. *Pre-incident risk assessment and management should be conducted*. While currently rare, the hostile use or 'weaponisation' of biotechnology is likely to become more frequent in the future. Security and intelligence communities will need to develop better relationships with the biotech sector to both reap possible benefits and manage potential risk.

3. *Measures must be established to respond to the challenges posed by emerging technologies.* The regulation of airspace, manufacturing standards and sales protocols are ways of ensuring the safe use of drones. Comprehensive responses require coordination. The UK, for example, is working towards the establishment of a national biosecurity strategy through collaborations with academia, industry partners and law enforcement agencies.

4. *Technological policy needs to be calibrated, understanding both the capabilities and limitations of new technologies.* The market often makes bold promises regarding the capabilities of technological innovation. In practice, however, new technologies tend to fall short in terms of user experience. For instance, exercises show that counter-drone systems are less effective than advertised.

5. *Civil society should be involved in efforts to expose fake news*. Involving non-governmental organisations can help establish public trust in government-led initiatives. For example, the Latvian government has engaged ethnic Russian speakers and online ‘influencers’ to reach intended audiences more effectively.

6. *Media relations are key to effective fact-checking*. A study by the Digital Forensic Research Lab showed that only 1% of those who follow websites which spread disinformation visit fact-checking websites. Debunking online hoaxes therefore needs to involve the engagement of relevant audiences through effective media relations.

7. *Regional organisations must be involved in efforts to counter disinformation.* For example, an EU initiative recently assembled an expert group to discuss best practices. A project by the NATO StratCom Centre of Excellence brings together eight Baltic nations twice a year to share thoughts on the vulnerabilities, best practices and common hostile narratives associated with disinformation campaigns. ASEAN should take similar measures.

## Session 2: Governing Difference

### The Corruption of Capitalism: Why Rentier Capitalism and the Growing Precariat are Threats to Social Stability

**Guy Standing**, *Professorial Research Associate, School of Oriental and African Studies, University of London*

1. The rise of finance and multinational corporations under the neoliberal economic order created a system of rentier capitalists, whereby large portions of income from property (physical or intellectual) went into the hands of a few.

2. The neoliberal economic model also encouraged the commodification of education systems, which now focus on preparing individuals for the workforce, while reducing the civic role of education and hindering the development of critical and well-informed citizens. Precariats generally lose their political, cultural, civil, social and economic rights, as they are unable to articulate their needs within society.

3. Precariats are largely made up of individuals who experience low wages and/or insecure work conditions, and have been habituated to accept their predicament. Others may experience income falling in real terms and increasing credit debt.

4. The precariat class can be divided into three categories: (a) the Atavists, or low-wage working class people tending towards neo-fascist and populist politics; (b) the Nostalgics, immigrants with no sense of home who will react when pressed; and (c) the Progressives, educated yet debt-laden individuals with no sense of hope, but may be more likely to participate politically and mobilise to react against capitalists.

5. Basic income is therefore important, as it would provide the precariat class a sense of security and prevent social instability. States should be cognisant of low-income earner difficulties, and produce an integrated strategy to empower the precariat.

### Governing Difference
**Tim Soutphomassane**, *Race Discrimination Commissioner, Australia*

1. Australia is a successful model of multiculturalism and cultural diversity, where half of the Australian population is first or second generation migrants. It was the first country to be recognised as "multicultural" in official terms, and citizens are guaranteed opportunities regardless of their backgrounds.

2. With the diversity observed within Australia, cultural integration is a key function of Australia's overall multicultural policy, which was termed the "family of the nation". Individuals from ethnic groups are not expected to abandon their cultural heritage, while still maintaining a secular national identity.

3. Multiculturalism in Australia is different from that practised in other states. For example, it varies from France's assimilationist model where the expression of cultural identity is left to the private realm and subordinate to the secular French identity. It is also different from the United Kingdom's integrationist "community of communities" approach, which suggests that each community can maintain their respective culture and beliefs, while not necessarily interacting with each other.

4. Racism is a key challenge. The Australian indigenous population in particular faces disparities in healthcare provision, access to jobs and education services. Racism in Australian society is reflected in the preference for Anglo-Celtic heritage within government and corporate leadership roles.

5. There are legal and non-legal tools for combating racism. Legal means include the Racial Discrimination Act of 1975, a legislative mechanism to mediate disputes. Non-legal means include the state's National Anti-Racism Strategy, which focuses on public awareness, youth engagement and education resources.

6. Contemporary debates within Australia include the resurgence of xenophobia by far-right groups and contestation over the amendment or repeal of Section 18C of Australia's Racial Discrimination Act. Section 18C makes it unlawful to commit an act which is reasonably likely to "offend, insult, humiliate or intimidate" another because of their race or ethnicity. The article also arguably limits the right to free speech.

### Scholarship and Urban Policies beyond Diversity
**Ayse Caglar**, *Professor, Department of Social and Cultural Anthropology, University of Vienna*

1. Differences between ethnic and religious groups may reduce societal solidarity, threaten social cohesion and foment social fragmentation. On the other hand, diversity can also be an asset, whereby group differences can be bridged and interactions encouraged. The challenge for governments is to govern cultural and economic differences between groups to maintain social cohesion, which is crucial for economic prosperity and security.

2. Cities, however, have become strategic sites for the generation of wealth, investment, trade and innovation. The restructuring of capital may affect how diversity is valued

within respective societies. In this regard, migrants and refugees should be leveraged as urban resources that can contribute to a city's economic competitiveness.

3. New analytical vocabulary and a conceptual network can capture the relationship between migrants and cities in urban redevelopment. For example, using the terms "displacement" and "emplacement" would focus on the processes underlying migration, while the word "sociability" implies commonality between groups.

4. Theories from migration and policy studies have largely been developed from the particular experiences of megacities or metropoles. Researchers and policymakers should pay more attention to the experiences of cities of different sizes, scales and levels of economic and political power.

5. It is pertinent to address inequalities between cities and the governance of diversity in relation to: (a) the interrelated processes of wealth generation; (b) urban redevelopment; (c) increasing disparities; and (d) migrant settlement.

6. Greater urban diversity presents various challenges. First, increased racism-diversity narratives may portray migrants or certain ethnic groups as impoverished or lagging behind.

## Syndicate Discussion

1. *Chronic economic insecurity in segments of society presents significant challenges*. While the definition of 'precariat' may differ from country to country, the term generally describes individuals who have few life options and hold socioeconomic grievances. Populist political movements and even extremist groups may exploit these vulnerabilities.

2. *The introduction of a basic income could ensure economic security.* As real wages stagnate and purchasing power declines, existing income distribution must be refined. Pilot studies show how social cohesion is strengthened through a guaranteed basic income.

3. *Policymaking needs to pay better attention to voices from below*. Societies that appear homogeneous on the surface can host internal differences. Misunderstanding dynamics on the ground may result in inappropriate or misdirected policy. Evidence-based research is crucial. For example, naturalisation indicators and statistics, coupled with surveys, may be used to assess whether social cohesion policies are effective.

4. *Legislation is an effective tool for regulating behaviour in terms of inter-ethnic relations*. In Australia, the racial discrimination law initially granted indigenous people with a "native" title. In the post-1975 era, the country has added legal provisions that safeguard against racial discrimination. Freedom of speech is therefore not absolute and may be restricted if it impinges on the freedom of others. Legislation prevents the ability to commit anti-social acts with impunity.

5. *Disinformation creates excessive fear of foreign interference that could potentially upset domestic interracial relationships.* Rumours and conspiracy theories can stoke sectarian tensions and undermine the effectiveness of integration efforts in multicultural societies. Practitioners should take care to prevent unjust treatment of any particular ethnic group resulting from the manipulation of foreign influence.

# Session 3: Terrorism and its Futures

## Radicalisation Spiralling Effects: The Interconnectedness of Different Forms of Extremism

**Julia Ebner**, *Research Fellow, Institute for Strategic Dialogue, United Kingdom*

1. The narratives of far-right and Islamist extremist groups, such as the English Defence League (EDL) and Hizb ut-Tahrir, are often similar in form and style. Online posters used as propaganda tools by these organisations rely on the same visual elements. References to pop culture and video games abound in both.

2. In terms of message delivery, these organisations often present themselves (and the people they claim to represent) as victims. They both promote the idea of an inevitable war between Islam and the West, Muslims and non-Muslims.

3. Strategies and tactics reveal further connections. Both types of group aim to polarise society and reap the fruits of discord and division. The "weaponisation of everyday life", illustrated by the use of mundane objects such as cars in terrorist attacks, has been observed in operations led by "lone wolves" belonging to both types of organisation.

4. Recruiters of each side target the same audience, i.e. young and often disaffected people. Cases of US neo-Nazis converting to Islamist militancy are examples of the interplay between the two ideologies. In addition, demonstrations and attacks carried out by members of far-right and Islamist groups tend to happen within a short timeframe, which suggests a possible correlation.

## From Memes to Marches: How Boots-on-the-Ground Events in 2017 Fractured the US Radical Right

**Susy Buchanan**, *Editor, Intelligence Project, Southern Poverty Law Centre, United States*

1. A sharp spike in hate incidents was observed in the days preceding Donald Trump's Presidential Inauguration in January 2017. Violent outbursts have also become frequent during extremist rallies in US cities such as the "Unite the Right Rally" held in Charlottesville, Virginia, in August 2017. A vehicular attack from a rally participant during the event killed one protestor and injured 19 others.

2. The Charlottesville clashes acted as a wake-up call for the tech world, and social media companies such as Facebook have since become more aggressive in fighting online hate speech. Within days of the rally, white supremacist accounts were suspended and extremist content was removed.

3. However, new rallies were carried out after Charlottesville. For example, the National Socialist Movement (NSM), one of the largest extremist groups monitored by the SPLC, demonstrated in Newnan, Georgia, in April 2018 to celebrate Adolf Hitler's birthday. Despite such incidents, the apparent momentum built by far-right groups during the summer of 2017 seems to be fading.

4. The SPLC has developed a three-pronged action plan. First, its Teaching Tolerance project aims to provide educators in US schools with various resources that reduce prejudice and promote understanding. Second, the SPLC collects evidence and takes

legal action against hate groups and their leaders. Third, the centre monitors the activities of more than 1,600 domestic extremist groups. Collaboration between the SPLC and law enforcement takes the form of training and information sharing.

## The Future of Terrorism in Southeast Asia: Some Preliminary Thoughts

**Kumar Ramakrishna**, *Associate Professor, Head of Policy Studies and Coordinator of the National Security Studies Programme, RSIS*

1. Contemporary violent extremism in Southeast Asia was infamously illustrated by Jemaah Islamiyah (JI), an Indonesia-based organisation established in the 1990s which conducted a series of large-scale attacks throughout the 2000s. New actors have since emerged, as reflected by follower of the so-called Islamic State (IS) and insurgent factions involved in the siege of Marawi in Mindanao, Southern Philippines from May to October 2017.

2. The ideology of groups such as Al-Qaeda (AQ) and IS is based on the idea of an all-out war with the US and its allies on the one hand, and the Muslim world on the other. Extremist ideologues consider the citizens of democratic systems to be responsible for the actions of their leaders, which they believe legitimises their indiscriminate attacks.

3. Future attacks in Southeast Asia are likely to be caused by local networks acting on behalf of IS and foreign fighters returning from overseas conflict zones. The threat also comes from “self-radicalised lone wolves”, i.e. individuals inspired by terrorist organisation propaganda but showing little or no operational connections with other militants.

4. In order to build regional resilience, initiatives are required to favour the implementation of peace and counter Islamophobia. The need for better governance is salient in war-torn areas such as Mindanao, where militant groups have long been active.

## Syndicate Discussion

1. *Policymakers need to examine non-violent extremism according to the laws of the country*. Organisations such as the Hizbut Tahrir Indonesia (HTI) do not overtly incite their followers to violence, but advocate problematic views such as a rejection of democracy and the establishment of a caliphate. Global developments may also tip non-violent extremists towards violence.

2. *Current legislation against hate speech has yet to catch up with conceptual literature*. Psychological studies have shown repeated denigrations of out-group members can influence in-group members to view outsiders as lesser human beings. Some extremist groups are careful not to cross the line into incitement or hate during public speeches and through the circulation of extremist material.

3. *There is a need to avoid simplistic explanations of radicalisation, such as attributing its growth to poverty as a key factor.* The propensity for radicalisation should be evaluated through three levels of analysis: (1) Macro (structural-level); (2) Meso (organisational-level, such as institutional culture, cultural perspectives and biases); and (3) Micro (individual-level, such as emotional and psychological considerations).

4. *Assessing claims of remorse among returning foreign fighters is challenging*. Some returnees may have been led astray and regretted decisions soon after joining an extremist organisation abroad; others may be pretending this is the case. Intelligence

and information sharing is crucial for building an accurate picture of a given individual's activities in order to inform appropriate responses.

5. *Radical groups have exploited loopholes in the US legal system*. Broad freedoms of speech in the US have allowed hard-line groups to promote their rhetoric while avoiding sanction. Legally grey tactics such as doxing (the act of researching and broadcasting private or personally identifiable information about an individual or organisation) are commonly employed by groups such as Antifa in the US against their opponents. They also use unregulated cryptocurrencies such as Bitcoin to fund their cause.

## Session 4: Cybersecurity: Boundaries and Securities

### How Japan is Closing a Cybersecurity Gap Toward Tokyo 2020

**Mihoko Matsubura**, *Adjunct Fellow, Pacific Forum, Japan*

1. There is currently a global shortage of cybersecurity talent. Projections by research firm Frost & Sullivan estimate a deficiency of 1.5 million cybersecurity professionals by 2020. Japan's shortfall of IT professionals relative to demand is projected to increase to almost 200,000 people over the coming years. This presents challenges leading up to the Tokyo Olympic Games in 2020.

2. Initiatives focusing on cybersecurity, principally from the Ministry of Economy, Trade & Industry (METI) and the Ministry of Internal Affairs & Communications (MIC), aim to tackle the human resource challenge. METI worked together with information technology agencies to establish the Industrial Cyber Security Center of Excellence (ICSCoE) in 2017. ICSCoE seeks to cultivate expertise in the protection of critical infrastructure and manage possible conflicts in Information Technology (IT) and Operational Technology (OT).

3. Government-sponsored education and training programmes for the next-generation of professionals include a one-year hackathon (i.e. SecHack 365) for Japanese students under 25 years old, as well as the Cyber Defense Exercise with Recurrence (CYDER) exercises for 3,000 central and local municipal government officials.

4. In preparation for the Tokyo 2020 Olympic Games, cyber exercises such as Cyber Colosseo have been conducted by the National Cyber Training Center for the Organising Committee of the Olympic and Paralympic Games. The aim was to simulate potential cyberattacks on Tokyo 2020 and review and enhance defensive capabilities with red-teaming scenarios, which foster team-building between security personnel and relevant organisations.

5. Private sector initiatives are also crucial for cultivating interest for cybersecurity technology and R&D among Japan's younger generation. Industry efforts for cybersecurity training also involve the establishment of a cross-sectoral committee for human resource departments to close cybersecurity gaps. Such initiatives are in line with Japan's new cybersecurity strategy in 2018.

## Cybersecurity Cosmos: Boundaries and Priorities

**Greg Austin**, *Professor, Australian Centre for Cyber Security, University of New South Wales (Canberra), Professional Fellow, East West Institute, Australia*

1. The dawn of the cyber age is almost cosmic in scale. Cybersecurity professionals now discuss the security of cyberspace in a twenty-year timeframe. The vast cyber landscape remains vulnerable as criminals and nefarious actors constantly breach its porous borders.

2. National cyber security is heavily dependent on international collaboration. Cyberspace can be described as a 'cosmic canvas' in which national policy and international relations strive for effective security. At the national level, protection problems in the cyber universe are increasingly scaled. Therefore, the importance of upholding robust national cyber security is heavily dependent on international collaboration.

3. The cyberspace landscape is dynamic. While humans currently control cyberspace, the rapid maturing and advancement of artificial intelligence and quantum computing will present new challenges to national security in the future. The scientific capabilities humans are developing for cyberspace (e.g. artificial intelligence and quantum computing) remain a key concern due to fears that such technologies may represent a fundamental threat to human security.

4. Three intractable problems in cyberspace present pertinent future challenges for the global community. Cybercrime, critical infrastructure protection, and content control all require strategies such as the prosecution of cybercriminals and the protection of critical infrastructure against protracted and sustained attacks.

## The Blurred Boundaries between Cybercrime and National Security

**Lior Tabansky**, *Head of Research Development, Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv*

1. The boundaries between cybercrime and national security are becoming increasingly blurred. Both state and non-state actors can work across a spectrum of power. For instance, cyberattacks by the Mabna Institute in Iran (which targeted 176 universities across 21 countries in 2017) were classified as a state-sanctioned cybercriminal operation even though they originally appeared to be a non-state sponsored cyber-attack.

2. The ambiguity of threat actor attribution and the organisational hierarchy of state response can lead to a defence impasse. It is crucial to note the crime-state nexus is a gamut rather than binary, as state-sanctioned cybercriminal attacks commonly utilise all available resources to achieve national goals. Cybercrime is capable of eroding a sense of security in society over a prolonged period of time and is therefore increasingly viewed as a national security threat.

3. Cybercrime as a Service (CaaS) will play a prominent role in the future of cybercrime as cooperation among criminal elements and hostile entities evolves over time. The online marketplace will see companies such as internal security contractors and private corporations marketing cyber services to state and non-state actors. The future may see increased outsourcing of projects to online marketplaces such as the dark web.

4. Nation states do not have complete situational awareness in cyberspace, which produces ambiguity and contributes to the defence impasse. Future advancements in technology may allow law enforcement to respond in ways that minimise damage and subvert attacks in order to gain enhanced situational awareness in cyberspace.

## Syndicate Discussion

1. *Cybersecurity is a global issue requiring cooperation and collaboration between nation-states*. Japan, for example, provides training for incident responses and consultation for the creation of robust national-level cybersecurity policies for ASEAN member states. Under the current administration, Japan is also pushing to expand existing defence cooperation with countries such as the US, UK and Australia, while also creating dialogues with countries such as Israel, Estonia and France.

2. *Strategies for cyber deterrence*. Cyber deterrence consists of punishment and denial. Deterrence by punishment involves direct attacks against the perpetrator before a malicious cyber incident is carried out. Deterrence by denial is a strategy of preventing cyberattack through pre-emptive measures such as regulation and legislation to prevent malicious activities in the cyberspace.

3. *Innovation is essential for more effective cybersecurity*. Israel has established a strong culture of innovation through high-level connectivity between sectors. As Israeli citizens often maintain more than one career simultaneously (for example, professors not only teach in universities but may also run their own companies), they can better understand and keep abreast of cross-sectoral issues and innovation which leads to more effective defence and cybersecurity.

4. *Attributing cyberattacks is challenging even if tactics and techniques are clear.* Multiple actors may be involved in a single attack, which may also be the result of combined efforts by perpetrators from different countries.

5. *Measures against cyberattacks.* The economic cost and political value of cyberattacks should be considered in crafting possible preventive measures such as the employment of kill-chains, air-gapping and/or cyber diplomacy.

6. *Cybersecurity policy needs to be granular, crafting clear definitions of cyber threats*. Broad definitions and implementation of policies result in inappropriate solutions. Addressing the proliferation of online child pornography, for instance, is significantly different from critical infrastructure protection. Cybersecurity policies need to tailor priorities according to the specific issue at hand.

# Session 5: Case Studies

## Immigration and Integration: Key Sources for Development

**Sofia Appelgren**, *Founder, Mitt Liv, Sweden*

1. Social entrepreneurship is critical for tackling issues that have not been addressed by governments. The successful integration and inclusion of migrants has the potential to inject new energy into aging Nordic societies, fuel economic progress and reinvigorate ailing welfare systems.

2. The current integration system in Sweden is built around accommodating refugees, which is a process that slows down integration for other migrant groups. High taxation rates in Sweden also create a common mind-set that government must take responsibility for solving all social problems. While several studies show that Sweden excels at integration, access to its labour market is a huge challenge for most immigrants. It can take many newcomers from five to nine years to find work.

3. Almost 8 out of 10 jobs in Sweden are obtained through contacts and professional networks, which play an integral role in job allocation. Without access to these networks or from recognised schools in Sweden, immigrants struggle to find employment. Sweden thus possesses an inherent conundrum, where there are open doors into the country for immigrants but closed doors that bar entry into the labour market.

4. Though concentrating on integration is essential, it is important to focus on inclusion and consistent interaction. The lack of state attention towards inclusion has been met by a rise in social enterprises, such as Mitt Livs, an organisation that offers mentorship, builds partnerships, professional networks, and aids with recruitment by including and integrating migrants. It also consults with organisations on instituting more inclusive practices in the workplace. These initiatives aim to create more space for interaction with a direct emphasis on fostering an inclusive society.

5. There is also a need to engage with the nearly 35,000 unaccompanied minors who have entered Sweden since 2015. Mitt Livs has worked closely with universities to engage newly arrived young people, prepare them for further educational opportunities and integrate them into Swedish society by introducing them to Swedish culture, norms and practices.

## Understanding and Managing the New Dimensions of Emerging Threats and Complex Risks

**Rebecca Nadin**, *Head, Risk & Resilience Programme, Overseas Development Institute, United Kingdom*

1. Risk is essentially about how we perceive outcomes. Socio-economic pathways are development and security choices which can create or modify threats and risk. These pathways give rise to complex threats and interact with those threats to make risky and uncertain outcomes. They create trade-offs and emerging threats.

2. Critical threats include geopolitical volatility, pandemics, shifting population dynamics, the information ecosystem and cyber fragilities, international criminal/terrorist networks, climate change, and financial system instability. Such threats are often non-diversifiable, transboundary, intergenerational, transitional (i.e. leading to major

societal transitions) and interact with each other to create layered risks. States may need to start rethinking approaches to managing these new dimensions through a better understanding of risk tolerance, uncertainty and trade-offs.

3. Climate change is a multi-dimensional, transboundary risk. Cities are becoming more vulnerable to the impact of climate change due to high population density and extensive infrastructure development. Much existing infrastructure is not well adapted to current climate risks and poorly placed to deal with those anticipated in the future.

4. Building resilience requires a better understanding of the multi-dimensional risks of emerging threats. These include transitional risks (e.g. stranded assets, jobs, unmet resource demands); transboundary risks (e.g. regional trade and import dependencies, migration); layered threats and risks (e.g. international criminal networks and economic inequality colliding with climate change); intergenerational risks; and non-diversifiable risks.

5. Forging resilience also entails a need to set decision-making criteria to better study risk tolerance and a set of local context indicators to analyse the relevance of contemporary dimension threats. It also necessitates more effective engagement with new stakeholders, stronger trust networks and multi-discipline collaboration giving equal importance to both qualitative and quantitative analysis.

## Populism and its Discontents
**John Judis**, *Author and Journalist, United States*

1. Populism is a difficult term to define, and while populist movements share family resemblances, they tend to maintain distinctly different identities. Populism is predicated on the sentiment that elite classes are not willing to give in to the affordable, achievable demands of the people. Grievance often manifests on the left as contempt for corporate greed and extraordinary personal wealth. On the right, it tends toward sentiment targeting an offending third out-group which the liberal elite is accused of coddling while ignoring the demands of the people.

2. Populism often emerges following a breakdown of consensus among ruling elites regarding the way a country should be run. The American economic landscape has been transformed in the last few decades which has greatly impacted semi-skilled, working class Americans who have either been replaced by cheaper immigrant labour or seen their entire industry phased out and sent offshore.

3. While immigration has long been seen as a source of insecurity and discontent in the United States, the terrorism threat since 9/11 made it a hot button issue. When a populist gets into office, they follow one of three strategies. First is one of accommodation, where the goal is to integrate with the establishment and cease their populist agenda. The second option is declaring war on the system and attempting to undermine it from within. The last strategy is to enter office and take on the establishment head on through populist warfare. Donald Trump has embraced this strategy.

4. There is a strong sense of dislocation in smaller towns across America, resentment toward the elite, and a distinct contempt for big business. Populism is a warning signal of discontent and a breakdown of public consensus.

### Syndicate Discussion

1. *The effective integration of migrants.* In Sweden, civil society organisations complement governmental efforts by implementing community orientation programmes to help new migrants learn about Swedish laws.

2. *Populism and its impact on public trust.* Politicians must remain attuned to common sentiment and address potential discontent arising from certain policies in order to avoid losing public support. While many media outlets advance specific political agendas, balanced deliberation is essential to maintain trust in public institutions.

3. *Risk assessment tools are currently confined within national boundaries and examine risk factors in silos*. As different countries have different priorities, it is challenging for national governments to advocate for international solutions. For example, while Singapore has conducted effective mitigation measures against rising sea levels and flooding in urban centres, it may be difficult to apply similar measures elsewhere. A holistic view of risk, and regional and global collaboration are needed to improve risk assessment capability.

4. *Understanding a country's risk tolerance is vital for addressing challenges*. Indonesia's desire to transition from a fossil fuel to low carbon economy, for example, comes with trade-offs, as labour has traditionally been a greater concern for the nation than managing climate change. Risk assessments therefore need to consider the types of risks that a nation may be able to tolerate before devising steps to mitigate problems.

5. *Resilience in policymaking*. Ensuring resilience is challenging because threats evolve and may emerge in unexpected ways. Risk assessment can provide foresight capabilities to build resilience, which is iterative and cyclical in nature. However, the political cycles of many countries pose challenges to foresight.

## Lunch Discussion, Singapore's National Security Past, Present, and Future

### Society and National Security

**Norman Vasu**, *Senior Fellow and Deputy Head, CENS, RSIS*

1. Singapore's narrative of vulnerability derives from the way the state has interpreted past events, namely the Japanese occupation, independence from Malaysia in 1965, and race and religious riots in the 1950s and 60s. Through these events, Singaporean leaders have established that Singapore must not rely on others for its security; must manage resources effectively; and protect its multicultural social fabric. The nation's security priorities are: securing its sovereignty (protecting against external threats) and maintaining public order (ensuring communal tensions of the past do not resurface).

2. Singapore's national security narrative is concerned with addressing the following issues: (1) racial and religious fault lines; (2) xenophobia, and a growing culture of intolerance and offence taking; and (3) disinformation campaigns and deliberate online falsehoods. The "slow burning" nature of these issues may mean they flare up in the future if not handled carefully.

3. The state's emphasis on ensuring communal harmony is illustrated by the celebration of Racial Harmony Day in schools to instil the message in successive generations that racial harmony should not be taken for granted.

4. Moving forward, it remains to be seen if the narrative of vulnerability can be sustained because the notion of Singapore being constantly on high alert may not be feasible. Singapore may have to rethink how it conceives its past, as this could constrain how it views itself in the present and conceptions of the future. Perhaps Singapore's security narrative should shift from one of vulnerability to one of resilience, to induce a more positive outlook to the challenges faced.

## Terrorism and Radicalisation

**Shashi Jayakumar**, *Senior Fellow and Head, CENS, RSIS*

1. The threat to Singapore's national security from terrorism was illustrated in the Jemaah Islamiyah (JI) White Paper published by the Ministry of Home Affairs (MHA) in 2002. The discovery, arrest, and detention of extremists in 2001-02 has largely informed Singapore's approach to countering terrorism. However, the circumstances surrounding radicalisation and terrorism have evolved significantly since the JI arrests.

2. As illustrated by the arrest of Bangladeshi foreign workers in 2016, Singapore takes severe action against any radicalised individuals. A number of them faced trial in Singapore before being deported, despite not intending to commit violent acts within the country.

3. Singapore's security establishment recognises threats from external sources, as illustrated by the foiled Marina Bay rocket attack in 2017, and domestically, from self-radicalised Singaporeans.

4. Individuals detained under the Internal Security Act (ISA) go through intensive religious rehabilitation, which boasts a success rate of roughly 88%. However, the profile of those detained is changing and currently most are considered self-radicalised individuals who are proving harder to rehabilitate. Minister Shanmugam announced recently that roughly 75% of the self-radicalised individuals detained are yet to be released.

5. The pernicious effect of social media and exposure to ISIS propagandists since 2015 resulted in a significant increase of self-radicalised individuals. Profiles among those detained are also evolving, with more well-educated, younger offenders and the emergence of women becoming involved.

6. Confidence and resilience building efforts within religious communities in Singapore are crucial to ensure radicalised individuals are reported to authorities and communities support one another.

## Cybersecurity and Technology

**Benjamin Ang**, *Senior Fellow and Coordinator of the Homeland Defence and Cyber Security Programme, CENS, RSIS*

1. Singapore has an asymmetric threat landscape where 'defenders' have funding and manpower issues, while 'attackers' (who could be state actors or organised criminals) only need to succeed one in a thousand times to cause harm.

2. Malicious actors often use tactics such as 'spear phishing', which combines social media data and public information to target fraudulent emails to specific individuals. They may also exploit the hacking and shadow economies, and purchase denial of service capabilities on the dark web.

3. The four key threats identified in the Cyber Threat Landscape report issued by the Singapore Cyber Security Agency are: (1) ransomware; (2) defacement; (3) phishing; and (4) command and control servers (DDOS).

4. Ransomware attacks pose a serious threat as they affect both computers and phones, they are inexpensive to carry out and indiscriminate. Numerous cases of website defacement were reported in Singapore in 2016, and continue to pose risks to vulnerable business websites. Phishing involves emails embedded with dangerous links, which may download malicious software or obtain personal information. DDOS occurs when thousands of computers are taken over to launch an attack on a target, using a command and control server. Sixty such servers were found in Singapore's cyber space in 2017 alone.

5. Digital opportunity must be balanced with digital risk so states can fully benefit from technological advancement while remaining safe and resilient.

6. The most vulnerable vectors of data breach and cyber threat are mobile devices and Smart Nation infrastructure. As part of Singapore's Smart Nation initiative, transport, healthcare, government services, green living, and active aging (all enabled by smart devices, internet connected homes and infrastructure) are vulnerable to cyberattacks.

7. Singapore's law enforcement agencies see benefits in smart policing, particularly the use of networked CCTVs for situational awareness and gathering data for analysis and investigation. However, risks include policing devices themselves being cyber attacked, an over-reliance on cyber technology, and invasions of privacy.

8. Singapore takes the threat of disinformation campaigns, information warfare, and fake news very seriously. This was illustrated by the recent Select Committee on Deliberate Online Falsehoods, which examined threats to Singapore's cyber security and possible strategies for combatting them. Several CENS' staff members submitted papers and gave testimonies to the committee.

## Discussion

1. The main issue with Singapore's vulnerability narrative is one of sustainability. A sense of self should be based on confidence rather than continual fear.

2. Most self-radicalised individuals in Singapore since 2013 were groomed online, and used online platforms. The success rates for rehabilitation are to date much lower for individuals who were self-radicalised.

3. As IS has lost much of its territory, it is reinventing its narrative in two ways: (1) supporters explain away the loss of territory by claiming they were not pure in their actions; and (2) ideologues argue they must suffer losses before they can be ultimately victorious.

4. Profiles of radicalised individuals are highly varied, making it more challenging for rehabilitation strategies to be effective. For example, Singapore's Religious Rehabilitation Group (RRG) may only be useful for individuals who are religiously radicalised, but not others.

5. Many societies have lost the ability to articulate a narrative which provides sufficient meaning and motivation for its citizens. This is why extremist groups and ideologies become so persuasive. Therefore, it is crucial that policy makers think about strategies apart from religious deradicalisation, such as disengagement and inter-faith dialogue.

## Distinguished Dinner Lecture

The Boundaries of National Security: Recent History, Global Trends and Emerging Priorities
**Michael Shoebridge**, *Director, Defence and Strategy, Australian Strategic Policy Institute, Australia*

1. The current global security landscape has been shaped by major developments, including the end of the Cold War, the rise of transnational terrorism, the growing importance of cybersecurity, the return of state-based threats, and power-balance changes to the international order.

2. A number of contemporary security priorities have emerged from this evolving global environment: The changing nature of states; the consequences of rapid military modernisation; internal political and societal tension; implausible denial as a form of power projection; and strategic and economic advantage sourced from coming waves of internet technologies. Balancing primary and national security is the responsibility of governments as well as the corporate sector and local communities.

3. New approaches to security partnerships that combine technological, strategic and economic considerations are required to address these emerging priorities. Effectively coordinated public-private collaborations with technology companies and universities can help design constructive policies and regulations, even as governments strive to balance privacy and security, while creating economic conditions conducive to innovation in the corporate sector.

4. Multilateralism is crucial to addressing these emerging priorities, which have both domestic and international implications. For example, while counterterrorism requires domestic partnerships among state agencies, international cooperation between security, military and law enforcement agencies is also essential. Multilateral institutions should be strengthened to meet their evolving roles, engage corporate actors, and for governments to leverage them effectively.

Discussion

1. Malicious actors may be more technologically advanced than law enforcement agencies as state institutions value stability and are often reluctant to adapt. Greater flexibility will be required to keep pace with savvy transnational criminals.

2. The manipulation of social media has grown increasingly sophisticated and disinformation campaigns threaten to undermine the resilience of societies. Decades of relative peace and prosperity may weaken a societies' ability to recover from crises. Legislation aiming to improve transparency should be part of the solution to safeguard decision-making processes and public opinion from covert outside influences.

3. Populist movements and leaders gain prominence by offering simple prescriptions for the complex global problems that traditional institutions are struggling to comprehend and solve.

4. Extremists and organised criminals will continue to innovate and exploit emerging technologies. Currently, national legislatures are bound by certain limitations regarding the removal of online extremist content. Technological companies must be aware of the vulnerabilities of their platforms and necessary measures must be taken to avoid their misuse.

## Country Presentations

### *Singapore, Australia, Bahrain, Bangladesh, Belgium and Brunei Darussalam*

1. Two common national security threats were identified by this diverse set of nations. First, Islamic State (IS)-inspired terrorist attacks by home-grown extremists was cited as a major security concern. This included the increasing risk of online radicalisation. Singapore was particularly concerned about the change in terrorist tactics such as the combined usage of vehicle-attacks and rudimentary weapons.
2. Second, threats to national cyberinfrastructure was highlighted as a major security concern, including breaches of government databases by both state and non-state actors, cyber activism and illicit cybercrime.
3. Bahrain and Brunei Darussalam have somewhat different concerns with regards to terrorism. While the representative from Bahrain spoke of his country's vulnerability given IS-presence in neighbouring countries, the threat from Hezbollah was also a worry for the nation. Similarly, the representative from Brunei Darussalam saidrather than a direct threat from IS and Qaeda (AQ), IS-affiliated groups in Southeast Asia posed a greater risk to his country's national security.
4. Returning foreign terrorist fighters (FTFs) from IS-controlled territories are a major concern for Bangladesh and Belgium. Both representatives emphasised the need for strong domestic legislation and international information sharing to counter the threat from returning FTFs.
5. The representatives from Singapore and Australia emphasised the importance of horizon scanning for the effective planning of national security strategies. Australia, for one, prioritises 'technology foresighting' to better project future scenarios and identify opportunities for national security communications.

### *Cambodia, Chile, India, Indonesia, Jordan, Republic of Korea, Lao PDR, Malaysia, Myanmar, New Zealand, Norway, Pakistan, Philippines, Qatar*

1. Terrorism is a growing concern for a number of nations yet The dynamics of radicalisation, recruitment and financing vary across different contexts. For example, Cambodia noted that social media has been used by IS-affiliated groups in Southeast Asia to attract sympathisers and fund terrorist activities. India, on the other hand, emphasised extremist groups' exploitation of marginalised segments of society through propaganda.
2. Regional dynamics also feed into the growth of extremism. In Southeast Asia, new IS-affiliated groups are made up of members from neighbouring countries such as Indonesia, the Philippines and Malaysia.
3. Growth in transnational organised crime was also seen as a critical threat by these nations. This included human trafficking, trade in illicit goods, such as drugs and contraband, and money laundering. Some country representatives stressed these illicit activities intersect with other security threats, such as the use of funds to support home-grown terrorist cells.
4. Legislative and community-based approaches are important to tackle security threats. For example, Cambodia, India, Jordan, Laos, Pakistan and Philippines emphasised the importance of strengthening existing law enforcement frameworks to counter the threat of terrorism. India is working on fostering stronger partnerships with religious leaders and seminaries as part of community efforts to combat extremist ideology.
5. The country representatives also shared ongoing efforts to bolster national security ahead of large-scale international events. Korea has set up the International Police Cooperation Centre (IPCC) for better information sharing and incident-reporting prior to the PyeongChang Winter Olympic Games 2018. New Zealand is currently improving its security measures and emergency management arrangements in preparation for APEC 2021. Qatar is also developing its national resilience and cybersecurity based on international best practices to prepare for the FIFA World Cup 2022.
6. Other security threats outlined included the spread of misinformation, environmental degradation and political instability.

### *Sri Lanka, Switzerland, Thailand, Turkey, United Arab Emirates*

1. A common national security threat identified by these nations was again that of terrorism and violent extremism.
2. The national representatives also outlined various unique security threats they face. Turkey, for example, sees itself as confronted by a transnational Islamic social movement, which adopts a long-term strategy that includes infiltration into state institutions and the manipulation of public opinion. Sri Lanka and Switzerland noted that environmental and cybersecurity concerns are becoming increasingly challenging.
3. Switzerland emphasised that responses are shaped by historical experience, national culture and the political system of the country in question. Sri Lanka proposed a multi-pronged counteraction strategy built on regional and global engagement. All of the present nations acknowledged the need for better international cooperation and collaboration to tackle contemporary national security challenges.

## Day-to-Day Programme

## Sunday, 6th May 2018

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

1500 – 1830hrs **Conference Registration for Speakers & Participants**
Venue : Conference Secretariat @ Libra Ballroom Level 1, MMS

1830 – 2100hrs **Cocktail Reception & Welcome Dinner**
Venue : Pool Garden, Pavilion, Level 5, MMS

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

## Monday, 7th May 2018

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**
**Mrs Josephine Teo**
*Minister, Ministry of Manpower;*
*Second Minister, Ministry of Home Affairs*

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

0950 – 1005hrs **Group Photo-taking *(Parallel Activity)***
Venue : Gemini Ballroom, Level 1, MMS

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

1100 – 1110hrs **Introduction to RSIS, CENS and APPSNO**
Venue : Marina Mandarin Ballroom (MMB)
Level 1, MMS

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

1110 – 1210hrs **Session I : Emergent Issues in Homeland Security**
Venue : MMB, Level 1, MMS

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

Speaker : **Arthur Michel**
*Co-Director*
*Centre for the Study of the Drone*
*Bard College*
*United States*

**Donara Barojan**
*Assistant Director*
*Research and Development*
*Digital Forensic Research Lab (@DFRLab)*
*Latvia*

**Piers Millett**
*Principal*
*Biosecure Ltd*
*United Kingdom*

1210 – 1300hrs **Lunch**

1300 – 1415hrs **Session I: Syndicate Discussions**

1415 – 1445hrs **Coffee Break**

1500 – 1800hrs **Heritage Tour**

1900 – 2100hrs **Networking Dinner**
Venue : AquaMarine, Level 4, MMS

## Tuesday, 8th May 2018

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

0900 – 1000hrs **Country Presentation on Homeland Security Management**
Venue : MMB, Level 1, MMS

Chairperson : **Benjamin Ang**
*Senior Fellow;*
*Coordinator, Cyber and Homeland Defence Programme, CENS, RSIS, NTU, Singapore*

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

1000 – 1100hrs **Session II: Governing Difference**
Venue : MMB, Level 1, MMS

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

Speakers : **Guy Standing**
*Professorial Research Associate*
*School of Oriental and African Studies*
*University of London*
*United Kingdom*

**Tim Soutphomassane**
*Race Discrimination Commissioner*
*Australia*

**Ayse Caglar**
*Professor*
*Department of Social & Cultural Anthropology*
*University of Vienna*
*Austria*

1100 – 1115hrs **Coffee Break**

1115 – 1230hrs **Session II: Syndicate Discussions**

1230 – 1330hrs **Lunch**

1330 – 1700hrs **Perspectivity Challenge**
**(on-going with coffee break)**
Venue : Pool Garden, Pavilion, Level 5, MMS

Facilitators : Perspectivity Foundation

1700hrs onwards **Free and Easy ( Networking Time )**

## Wednesday, 9th May 2018

0630 – 0845hrs **Breakfast**

Venue : AquaMarine, Level 4, MMS

0900 – 1120hrs **Country Presentation on Homeland Security Management**

Venue : MMB, Level 1, MMS

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

Presenters : By alphabetical order: ***Cambodia, Chile, India, Indonesia, Jordan, Korea, Republic of, Lao PDR, Malaysia, Myanmar, New Zealand, Norway, Pakistan, Philippines and Qatar***

1120 – 1130hrs **Coffee Break**

1130 – 1230hrs **Session III: Terrorism and its Futures**

Venue : MMB, Level 1, MMS

Chairperson : **Joseph Franco**
*Research Fellow*
*Radicalisation Studies Programme*
*CENS, RSIS, NTU, Singapore*

Speakers : **Julia Ebner**
*Research Fellow*
*Institute for Strategic Dialogue*
*United Kingdom*

**Susy Buchanan**
*Editor*
*Intelligence Project*
*Southern Poverty Law Center*
*United States*

**Kumar Ramakrishna**
*Associate Professor, Head, Policy Studies; Coordinator, National Security Studies Programme, RSIS, NTU, Singapore*

1230 – 1330hrs Lunch followed by FREE and EASY (Networking Time)

1330 – 1445hrs Session III: Syndicate Discussions

1445 – 1645hrs Coffee Break followed by FREE and EASY (Networking Time)

1645hrs Assemble at Hotel Lobby for Distinguished Dinner Lecture

**1730 – 1830hrs** **Distinguished Dinner Lecture: The Boundaries of National Security: Controlling the Scope and Understanding Emerging New Priorities**

Venue : Saffron Ballroom, Level 2, Equarius Hotel;
Resorts World Sentosa
Sentosa

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

Speaker : **Michael Shoebridge**
*Director*
*Defence and Strategy*
*Australian Strategic Policy Institute*
*Australia*

1845 – 1915hrs **Cocktail Reception**
Venue : S.E.A. Aquarium,
Resorts World Sentosa,
Sentosa

1930 - 2100hrs **Dinner**
Venue : Ocean Gallery in S.E.A. Aquarium,
Resorts World Sentosa,
Sentosa

2100 hrs **Transportation to Marina Mandarin Singapore**

## Thursday, 10th May 2018

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

0900 – 1000hrs **Session IV: Cybersecurity: Boundaries and Priorities**
Venue : MMB, Level 1, MMS

Chairperson : **Benjamin Ang**
*Senior Fellow;*
*Coordinator, Cyber and Homeland Defence Programme, CENS, RSIS, NTU, Singapore*

Speakers : **Mihoko Matsubara**
*Adjunct Fellow*
*Pacific Forum*
*Japan*

**Greg Austin**
*Professor*
*Australian Centre for Cyber Security*
*University of New South Wales*
*(Canberra);*
*Professorial Fellow*
*EastWest Institute*
*Australia*

**Lior Tabansky**
*Head of Research Development*
*Blavatnik Interdisciplinary Cyber*
*Research Center*
*Tel Aviv University*
*Israel*

1000 – 1115hrs **Session IV: Syndicate Discussions**

1130 - 1400hrs **Lunch Discussion: Singapore's Security and its Futures (CENS)**

Venue : Vanda Ballroom, Level 5, MMS

Chairperson : **Terri-Anne Teo**
*Research Fellow,*
*CENS, RSIS, NTU, Singapore*

Speakers : **Shashi Jayakumar**
*Senior Fellow;*
*Head, CENS*
*Executive Coordinator*
*Future Issues and Technology*
*RSIS, NTU, Singapore*

**Norman Vasu**
*Senior Fellow;*
*Deputy Head, CENS*
*Coordinator*
*Social Resilience Programme*
*RSIS, NTU, Singapore*

**Benjamin Ang**
*Senior Fellow;*
*Coordinator*
*Cyber and Homeland Defence*
*Programme CENS, RSIS, NTU,*
*Singapore*

1400hrs **Coffee Break followed by FREE and EASY (Networking Time)**

## Friday, 11th May 2018

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

0900 – 1000hrs **Country Presentation on Homeland Security Management**
Venue : MMB, Level 1, MMS

Chairperson : **Muhammad Faizal Bin Abdul Rahman**
*Research Fellow,*
*Cyber and Homeland Defence Programme,*
*CENS, RSIS, NTU, Singapore*

Presenters : By alphabetical order starting with host country:
***Sri Lanka, Switzerland, Thailand, Turkey and United Arab Emirates***

1000 – 1100hrs **Session V: Case Studies**
Venue : MMB, Level 1, MMS

Chairperson : **Gulizar Haciyakupoglu**
*Research Fellow,*
*Cyber and Homeland Defence Programme,*
*CENS, RSIS, NTU, Singapore*

Speakers : **Sofia Appelgren**
*Founder*
*Mitt Liv*
*Sweden*

**Rebecca Nadin**
*Head*
*Risk & Resilience Programme*
*Overseas Development Institute*
*United Kingdom*

**John Judis**
*Author and Journalist*
*United States*

1100 – 1115hrs **Coffee Break**

1115 – 1230hrs **Session V: Syndicate Discussions**

1230 – 1830hrs **Lunch followed by Free and Easy (Networking Time) ***

1830 – 1900hrs **Cocktail Reception**
Venue : MMB, Level 1, MMS

1900 – 1945hrs **12th APPSNO Certificate Presentation Ceremony**

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

1945 onwards **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

Mrs Josephine Teo
Minister for Manpower and
Second Minister for Home 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

Sofia Appelgren
Founder
Mitt Liv
Sweden

Greg Austin
Professor
Australian Centre for Cyber Security
University of New South Wales (Canberra);
Professorial Fellow
EastWest Institute (EWI)
Australia

Donara Barojan
Assistant Director
Research and Development
Digital Forensic Research Lab (@DFRLab)
NATO Stratcom Centre of Excellence
Latvia

Susy Buchanan
Editor
Intelligence Project
Southern Poverty Law Center
United States

Ayse Caglar
Professor
Department of Social and Cultural Anthropology
University of Vienna
Austria

Julia Ebner
Research Fellow
Institute for Strategic Dialogue
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

John B. Judis
Author and Journalist
United States

Mihoko Matsubara
Adjunct Fellow
Pacific Forum
Japan

Arthur Michel
Co-Director
Centre for the Study of the Drone
Bard College
United States

Piers D Millett
Principal
Biosecure Ltd
United Kingdom

Rebecca Nadin
Head
Risk & Resilience Programme
Overseas Development Institute
United Kingdom

Kumar Ramakrishna
Associate Professor and Head of Policy Studies;
Coordinator, National Security Studies Programme
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

Michael Shoebridge
Director
Defence and Strategy
Australian Strategic Policy Institute
Australia

Tim Soutphommasane
Race Discrimination Commissioner
Australia

Guy Standing
Professorial Research Associate
School of Oriental and African Studies
University of London
United Kingdom

Lior Tabansky
Head of Research Development
Blavatnik Interdisciplinary Cyber Research Center
Tel Aviv University
Israel

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 Chairpersons

CHAIRPERSONS

Muhammad Faizal Bin Abdul Rahman
Research Fellow
Cyber and Homeland Defence Programme
Centre of Excellence for National Security
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

Joseph Franco
Research Fellow
Radicalisation Studies 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

Terri-Anne Teo
Research Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Nanyang Technological University
Singapore

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

## List of Participants

| | |
|---|---|
| AUSTRALIA | Nigel McGinty<br>Head<br>Strategy and Joint Force Branch<br>Joint and Operations Analysis Division<br>Defence Science and Technology Group<br>Australia |
| BAHRAIN | Hamad Mohamed Alkhayyat<br>Director of Directorate Operations<br>Ministry of Interior<br>Kingdom of Bahrain |
| BANGLADESH | Mizanur Rahman Shameem<br>Director<br>National Security Intelligence<br>Bangladesh |
| BELGIUM | Jean Fontaine<br>Chief Superintendent<br>Belgian Federal Police<br>Belgium |
| BRUNEI DARUSSALAM | Awang Besar Ismail<br>Assistant Director of Operations<br>Brunei Research Department<br>Prime Minister's Office<br>Brunei Darussalam |
| CAMBODIA | Meas Sophearith<br>Assistant to the Chief of Army;<br>Deputy Director, External Operations Department<br>General Department of Research and Intelligence<br>Ministry of National Defence<br>Cambodia |
| CHILE | Julio Torres Gonzalez<br>Analyst<br>Direction of International and Human Security<br>Ministry of Foreign Affairs<br>Chile |
| INDIA | Alankrita Sinha<br>Assistant Director<br>National Security Coordination Secretariat<br>India |

| | |
|---|---|
| INDONESIA | Constantinus Yuki Nurwahyu Hono<br>Senior Analyst<br>State Intelligence Agency (BIN)<br>Indonesia |
| JORDAN | Emad Hamdi Abdel-Alzubi<br>Special Branch Director Deputy<br>Public Security Directorate<br>Jordan |
| KOREA, REPUBLIC OF | Bok-Soon Kang<br>Senior Superintendent<br>Director of Foreign Affairs<br>Intelligence Division<br>Korean National Police Agency (KNPA)<br>Republic of Korea |
| KOREA, REPUBLIC OF | Sunghoon Moon<br>International Mutual Assistance Officer<br>Foreign Affairs Bureau<br>Korean National Police Agency (KNPA)<br>Republic of Korea |
| LAO PDR | Bounkham Manivan<br>Deputy Director<br>Asia-Pacific Division<br>Intelligence Department<br>Lao PDR |
| MALAYSIA | Aminudin Bin Yahaya<br>Deputy Director<br>Research Division<br>Prime Minister’s Department<br>Malaysia |
| MYANMAR | Soe Paing<br>Commander of Division (4), Taunggyi<br>Special Branch<br>Myanmar Police Force<br>Myanmar |
| NEW ZEALAND | Catriona Robinson<br>Director<br>National Security Systems<br>Department of the Prime Minister and Cabinet<br>New Zealand |

NORWAY

Hilde Bohn
Chief Analyst
Department of Analysis and National Preparedness
Directorate for Civil Protection (DSB)
Norway

PAKISTAN

Muhammad Jafer
Director General
National Counter Terrorism Authority
Pakistan

PHILIPPINES

Restituto T. Santos
Assistant Director General for Counter-Terrorism
DVI National Intelligence Coordinating Agency
Philippines

QATAR

Ali Mohammed Al-Ali
Deputy Executive Director of Security
Supreme Committee for Delivery & Legacy
Qatar

SINGAPORE

Alvin Chia Yong Ping
Assistant Director
Operations Planning & Technology Department
Security Division
Jurong Town Corporation
Singapore

SINGAPORE

Chin Piao
Programme Manager (Human Science)
Future Systems & Technology Directorate
DSO National Laboratories
Singapore

SINGAPORE

Chin Yen Yen
Senior Assistant Director
Policy and International Relations
National Security Coordination Secretariat
Prime Minister's Office
Singapore

SINGAPORE

Bernard Chua Tee Chiang
Senior Assistant Director
Economic Security and Resilience Division
Ministry of Trade and Industry
Singapore

SINGAPORE

Cui Shaowen
Deputy Director
Research & Strategy Management Division
Ministry of National Development
Singapore

SINGAPORE

Seraju Deen
Assistant Director
Security Department
Port Systems Division
Maritime and Port Authority of Singapore
Singapore

SINGAPORE

Maxmillion Goh Wei Shin
Commander, Tactical Air Support Group;
Head, Operations Development Group
Ministry of Defence
Singapore

SINGAPORE

Ho Siak Khong, Bernie
Deputy Director
Middle East, North Africa and Central Asia Directorate
Ministry of Foreign Affairs
Singapore

SINGAPORE

Hong Ying Quan, Lucien
Deputy Director
Africa Branch
South Asia and Sub-Saharan Africa Directorate
Ministry of Foreign Affairs
Singapore

SINGAPORE

Hsu Yu Chih, Tommy
Deputy Director
Security and Emergency Planning Office
Ministry of Education
Singapore

SINGAPORE

Huang Shao Fei
Director
Cybersecurity
Land Transport Authority
Singapore

SINGAPORE

Koh Tee Meng
Assistant Director
Operations, Investigation Policy and Training
Criminal Investigation Department
Singapore Police Force
Singapore

SINGAPORE

Lee Kim Hwee
Director
System Control Department
Power System Operation Division
Energy Market Authority
Singapore

SINGAPORE

Lee Wei Ling, Connie
Deputy Director
Communications and Engagement Office
Cyber Security Agency of Singapore (CSA)
Singapore

SINGAPORE

Grace, Leong Ying Wai
Senior Assistant Director
National Security Research Centre
National Security Coordination Secretariat
Prime Minister's Office
Singapore

SINGAPORE

Liau Chie Kiong
Senior Deputy Director
Network and Service Resilience
Info-communications Media Development Authority
Singapore

SINGAPORE

Lim Kwong Fei
Head
Strategic Procurement Unit
Resource Management Directorate
Ministry of Finance
Singapore

SINGAPORE

Lim Chern Choong, Wesley
Chief Instructor
Civil Defence Academy
Singapore Civil Defence Force
Singapore

SINGAPORE

Lim Teck Hong
Senior Assistant Director
Cybersecurity Policy
Cyber Security and Resilience Division
Ministry of Communications and Information
Singapore

SINGAPORE
Lim Kah Keng
Head
Army Current Operations Group
Ministry of Defence
Singapore

SINGAPORE
Lim Huay Wen
Branch Head
Naval Intelligence Department
Ministry of Defence
Singapore

SINGAPORE
Laurence Lim
Superintendent 1A (APF)
Assistant Vice President;
Senior Commanding Officer
Certis CISCO Auxiliary Police Force
Singapore

SINGAPORE
Ng Chee Siong
Head
Operations Policy and Development Branch;
Prosecution Branch
Intelligence and Investigation Division
Singapore Customs
Singapore

SINGAPORE
Winston, Ong Eng Siong
Assistant Director
National Security Engineering Centre
Defence Science and Technology Agency
Singapore

SINGAPORE
Ong Kim Hock, Nicholas
Senior Consultant
Government Technology Agency
Singapore

SINGAPORE
Ooi Tjin Kai
Deputy Head
Naval Operations
Naval Operations Department
Ministry of Defence
Singapore

SINGAPORE
Pang Tzer Yeu
Director (Plans)
Defence Cyber Organisation
Ministry of Defence
Singapore

SINGAPORE

Peh Chye Hock, Thomas
Deputy Director
Curriculum and Training
Institute of Safety and Security Studies
Centre for Protective Security Studies
Singapore

SINGAPORE

Peng Kah Poh
Director
Joint Operations Department
Public Utilities Board
Singapore

SINGAPORE

Winson, Sheo Boon Chew
Head
Field Security Branch
Military Security Department
Ministry of Defence
Singapore

SINGAPORE

Soh Hwee Fun, Ivy
Assistant Director
Operations Management Branch
Singapore Prison Service
Singapore

SINGAPORE

Maran s/o V K Subrahmaniyan
Deputy Director
Enforcement Division
Immigration & Checkpoints Authority
Singapore

SINGAPORE

Tan Fang Qun
Director (Operations Group)
Joint Operations Division
Ministry of Manpower
Singapore

SINGAPORE

Tan Chang Wei, Elgin
Assistant Director (Intelligence Collection)
Intelligence Collection Branch
Singapore Prison Service
Singapore

SINGAPORE

Alvin, Tan Teck Kai
Head
General Staff
AETOS Auxiliary Police Force
Singapore

SINGAPORE

Tan Yuh Cherng
Executive Vice President/ General Manager
Training and Simulation Systems
ST Electronics
Singapore

SINGAPORE

Tang Gek Hsien
Senior Assistant Director (Investigation Development)
Joint Operations Management
Joint Operations Group
Ministry of Home Affairs
Singapore

SINGAPORE

Karen Teh
Senior Deputy Director
Cybersecurity R&D
National Research Foundation
Prime Minister’s Office
Singapore

SINGAPORE

Teo Soo Yeow
Deputy Head
Air Operations Department
(Strategies and Plans Group)
Ministry of Defence
Singapore

SINGAPORE

Tng Ban Chuan
Deputy Commander (Ground Operations Terminals)
Coastal Command
Immigration & Checkpoints Authority
Singapore

SINGAPORE

Toh Yew Piau, Adrian
Assistant Director
Police Intelligence Department
Field Collection Division
Singapore Police Force
Singapore

SINGAPORE

Toh Soon Teck
Senior Assistant Director
Capital & Major Investigations
Investigation Division
Central Narcotics Bureau
Singapore

| | |
|---|---|
| SINGAPORE | Chris, Voo Hong Ping<br>Deputy Director<br>National Maritime Operations Group<br>Singapore Maritime Crisis Centre<br>Singapore |
| SRI LANKA | Priyantha Senaratne<br>Commandant<br>Sri Lanka Military Academy<br>Sri Lanka |
| SWITZERLAND | Bruno Rösli<br>Deputy Head<br>Security Policy<br>Federal Department of Defence<br>Civil Protection and Sports<br>Switzerland |
| THAILAND | Wathanachai Thongprasert<br>Division Director<br>Division of Cyber Investigation<br>Thailand |
| TURKEY | Okan Dogan<br>Chief of Division<br>Turkish National Intelligence Organisation<br>Turkey |
| UNITED ARAB EMIRATES | Saif Al-Aryani<br>Director<br>Capability Building Affairs Directorate<br>Ministry of Defense<br>United Arab Emirates |
| UNITED ARAB EMIRATES | Khalifa Al Ghafli<br>Acting Director<br>Supreme Council of National Security<br>United Arab Emirates |

## 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.