Event Report

GOH KENG SWEE COMMAND AND STAFF COLLEGE SEMINAR 2017

CHALLENGES AND THE IMPACT OF CYBER THREATS AND TERRORISM ON NATIONAL SECURITY AND THE ROLE OF THE MILITARY

Report of a seminar jointly organised by:
Goh Keng Swee Command and Staff College (GKS CSC),
S. Rajaratnam School of International Studies (RSIS), and
SAF-NTU Academy (SNA)

5-6 October 2017
SAFTI Military Institute
Singapore

Editor:
Eugene Mark

Rapporteurs:
Ng Chew Yee, Andre Foo Yong-De, Henrik Paulsson, and Eugene Mark

This report summarises the proceedings of the conference as interpreted by the assigned rapporteurs and editor from the S. Rajaratnam School of International Studies. The speakers and participants neither reviewed nor approved this report.

The seminar adhered to a variation of the Chatham House Rule. Accordingly, beyond the points expressed by the speakers in their prepared papers and in their remarks at question time, no attributions have been included in this conference report.

TABLE OF CONTENTS

Executive Summary	1
Opening Remarks and Keynote Address	2
Panel 1: Emerging Issues, Trends, and Implications of Cyber Threats	8
Panel 2: Confronting Cybersecurity Challenges	14
Panel 3: Evolving Threat of Terrorism	21
Panel 4: Countering the Threat of Terrorism — Strategies and Approaches	27
Plenary Presentations	34
Closing Remarks	36
List of Speakers and Chairs	41
About the Goh Keng Swee Command and Staff College	44
About the SAF-NTU Academy	44
About the S. Rajaratnam School of International Studies	45

Introduction

Since 2010, the Goh Keng Swee Command and Staff College (GKS CSC) has held an annual seminar that provides an important forum for participants to discuss issues of relevance to the education of military leaders. The seminar series also presents a unique opportunity for networking and professional exchange for both the participants and the expert speakers who are invited to share their thoughts.

GKS CSC Seminar 2017, titled "Challenges and the Impact of Cyber Threats and Terrorism on National Security and the Role of the Military", addressed an important challenge that is compounded by rapid technological advancements and the high levels of connectivity and porous borders in today's globalised world. The seminar involved a number of panel discussions that featured experts from the academic, military, and industry professional communities. The topics discussed included strategies that the military could adopt in responding to cyber and terror threats. Participants and speakers alike found the seminar engaging and useful.

Opening Remarks

Colonel Simon Lee Wee Chek
Commandant, Goh Keng Swee Command and Staff College
SAFTI Military Institute
Singapore Armed Forces

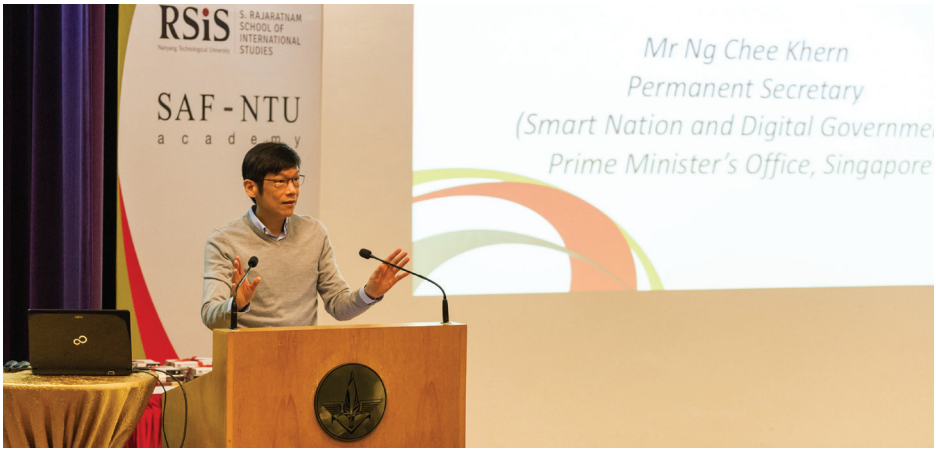
Colonel (COL) Simon Lee Wee Check began his opening address by highlighting the importance of the Goh Keng Swee Command and Staff College (GKS CSC) Seminar series in augmenting the learning of GKS CSC students on current security issues. He was encouraged that this year's seminar had attracted a mix of academics and industry as well as government professionals, who had rich insights to share on cyber threats and terrorism.

On cyber threats, COL Lee pointed out that the speed, reach, and impact of the threat had increased at a rate that no state could cope with. For instance, the "WannaCry" ransomware attack on 17 May 2017 was reported to have affected more than 230,000 computers in over 150 countries within a day. It disrupted the National Health Services in the United Kingdom and heavily affected businesses in Russia, Ukraine, India, and Taiwan. The threat was spotted by a British cybersecurity researcher only after two days. By then, an estimated loss of US$4 billion had been incurred worldwide. COL Lee warned that Singapore was not immune to cyberattacks. In April 2017, hackers attacked the networks of NTU and the National University of Singapore to steal government and research data. MINDEF and the SAF networks suffered similar attacks. While Singapore was fortunate that these

cyberattacks did not affect critical systems, the attacks were a stark reminder that cyber threats are real in Singapore.

On terrorism, COL Lee highlighted the rise of the tactic of using everyday objects to create menace and incite fear. This tactic was evident in incidents across Europe. A key incident of this nature in 2016 was the Bastille Day Attack in Nice, France, which killed 86 people. COL Lee said that significant resources were required to guard against such attacks, which would remain a challenge for most states. He also elaborated on the threat that returning fighters from Syria and Iraq would pose for Southeast Asia. The bombing of Jakarta in May 2017 and the siege of Marawi in the Philippines were examples of violent extremist presence in the region. COL Lee said the seminar sought to understand the nature of these threats and the role of the military in the wider national effort to counter them.

Keynote Address



Mr Ng Chee Khern
Permanent Secretary (Smart Nation and Digital Government),
Prime Minister's Office
Singapore

Noting that cyberattacks and terrorism were intractable challenges, Mr Ng Chee Kern put forth the following four propositions for participants to think about:

(i) Despite the differences between cyberattacks and terrorism, one similarity between the two is that they do not respect certain distinctions that militaries do. For one, perpetrators of cyber and terrorist attacks do not respect the distinction between peacetime and wartime, nor the difference between combatants and non-combatants. Another dimension that militaries respect but cybercriminals and terrorists do not is the idea of national boundaries. Essentially, cyber and terrorist attacks are transnational, making no distinction between the domestic and international domains. By holding on to these distinctions, militaries become less effective in addressing cyber and terrorist threats.

(ii) Addressing cyber and terrorist threats would entail expanding the scope of the military's capabilities and would involve technical expertise that most militaries do not yet possess. Using the historical analogy of innovation during the inter-war years, when militaries used the internal combustion engine to develop military air power capabilities, Mr Ng posited that the SAF was similarly placed at the start of an era where

significant and discontinuous capabilities must be assimilated by armed forces. As part of the larger process of adapting cyber capabilities from commercial entities, the SAF will face the challenge of integrating such capabilities into current operational structures.

In this context, Mr Ng addressed the common perception that the planning process of the Ministry of Defence (MINDEF) is structured and does not deal with real world problems, unlike that of other government agencies. He said there was some truth to this perception and acknowledged that the structured planning process of MINDEF and the SAF would bring about certain liabilities when dealing with adversaries with mindsets that they are not familiar with.

(iii) The military culture of centralisation has implications for the way militaries respond to cyber and terrorist threats. In the face of such threats, an effective solution is to decentralise the operational responses to the tactical levels. Although the decentralisation mindset has been emphasised in the SAF for more than two decades, it is not the natural way of doing things for the SAF and even for Singaporeans. Nevertheless, in order to be effective against cyber threats that move at the speed of light, there needs to be quick responses. Hence, the SAF has to develop the culture of trusting subordinates down the line to accelerate effective decision-making.

(iv) At the geostrategic level, both cyber and terrorist threats would make international relations more unstable as one of the key tenets of international relations is structured inter-state behaviour. Because states know the capabilities of one another to some extent, there is a certain stability between them, and the chances of strategic surprise are low. However, we are reaching an era where it is difficult to know the capabilities of other states. In such circumstances of uncertainty, states might be tempted to undertake pre-emptive action when under pressure.

In closing, Mr Ng pointed out that the United States had since 2013 declared cyber threats as the most serious security threat, ahead of terrorism. He noted that Singapore had never ranked one national security threat above another. However, from the SAF's perspective, cyber threats would be more familiar as the most serious of such threats tend to be state-based, and the SAF is used to dealing with state actors. Hence, Mr Ng noted, cyber issues are instinctively easier to grasp by the SAF. However, he added that the threat of terrorism was more serious owing to its potential to affect Singapore's social fabric.

Question-and-Answer Session

Responding to a question on how civilian agencies can work together with the military to address cyber threats, Mr Ng noted that different countries approach the threat differently. Some states might feel that the military should take on a wider role in protecting the whole country against cyber threats, even during peacetime. Other states believe that a military's cyber capabilities should only be for defending its own systems. Mr Ng said the SAF's contribution would depend on the extent to which it had built its cyber capabilities as well as the extent to which the civilian agencies, for their part, had developed their own cyber capabilities. Nevertheless, Mr Ng added that the best way for the SAF to deal with cyber threats would be to continue working closely with Singapore's Cyber Security Agency (CSA).

On the question of how Singapore would manage relations with friendly countries if there was a state-based cyberattack, Mr Ng replied that it would depend on Singapore's perception of its relationships. In order to operate well in a cyber threat environment, countries should not be too rigid about demarcating between friends and enemies, he said. Singapore should instead feel comfortable operating in a grey world, remaining friends with those that we know are attacking us and not taking offence easily.

One participant wanted to know what the aftermath scenario was likely to be in the event of a terrorist attack in Singapore. Mr Ng replied that the Singapore government had done a lot to ensure that normalcy would return in such an eventuality. The main task for the government was to make sure that the social fabric of Singapore would not tear apart. Mr Ng conceded that it was not possible to foresee the fallout with certainty as some individuals might act differently in the event of a terrorist attack from what they had claimed in public discussions. The aftermath scenario would also be dependent on who committed the act, the motivations behind it, the number of lives lost, and the amount of damage done.

The last question was centred on the key cyber threats to Singapore as it embarked on its "Smart Nation" initiative and how the government should prepare to make the country more secure. Mr Ng pointed out that cyber threats come from both external and insider sources. According to statistics, many security compromises originate from insider sources. To deal with insider threats, Mr Ng said we need to cultivate a good internal culture. As for external threats, the government, he noted, had begun to take stringent measures, such as localisation of sensitive data within the country. Nevertheless, there needs to be a balance between ensuring security and

keeping ahead of technological trends, he suggested. Within the Singapore government, he noted, there were some calling for a more permissive cloud policy because many digital capabilities were being built in the cloud domain today and Singapore could find itself marginalised if it did not avail itself of such technologies. Therefore, Mr Ng suggested, the SAF might need to consider being more flexible about how it classifies information.

Panel 1: Emerging Issues, Trends, and Implications of Cyber Threats

Assistant Professor Michael Raska
Military Transformations Programme, Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

Assistant Professor Michael Raska approached cyber threats from a military strategic perspective. He posed three propositions in his brief presentation. First, Asst Prof Raska addressed the question of whether military cyber capabilities could achieve political and strategic effects in the same way that conventional capabilities could. Sceptics, he said, would argue that military cyber capabilities cannot achieve political and strategic effects, transform regional power structures, or replace conventional military capabilities for coercion or deterrence. Using the example of the North Korean crisis, he noted that sceptics would argue that the political effects would be limited if North Korea threatened the United States with cyber weapons as opposed to nuclear weapons. On the other side of the spectrum, Asst Prof Raska noted, cyber proponents would argue that military cyber capabilities can be a force multiplier of kinetic operations, altering the character of future warfare. In their view, cyber weapons can be used to influence perception, behaviour, and the decisions of target audiences in real time. They can also play a denial role and create political outcomes without visible military commitments.

Second, Asst Prof Raska highlighted the issue of measuring military cyber capabilities and integrating them into existing force structures. The question was whether militaries should revise their doctrines, concepts,

and organisational structures entirely or integrate cyber weapons into their existing structures as a mere supporting element. Asst Prof Raska felt that deeper integration of cyber capabilities into the force structure would bring about more dependence on them, which in turn would translate into greater vulnerabilities. If that is the case, militaries must decide whether to go all the way to develop military cyber capabilities or trade away some of their cyber capabilities to reduce their vulnerabilities.

Third, Asst Prof Raska suggested that states with different strategic cultures would respond differently to the same technological disruption. In other words, the Chinese, Russians, and Americans would have different views on how to respond to a particular technological disruption. As different countries conceptualise cyber capabilities differently, there would be a difference in how they use or intend to use cyber capabilities.

Mr Matthias Yeo
Chief Technology Officer, Symantec Corporation
Singapore

Mr Matthias Yeo began by presenting some malware and ransomware statistics to illustrate the scale of cyber threats. He explained that Symantec Corporation in the past year had found about 401 million unique malware which were not replicated. Out of these, 89 per cent, or 357 million malware, were seen for the first time. In other words, an average of 1 million new malware are being written daily. In terms of ransomware, approximately 464,000 of them were detected during the past year. Mr Yeo noted that there was an upward trend in the ransom consumers paid out to perpetrators of ransomware: whereas two years ago the ransom was over US$200 per case, this year, it was about US$1,000. The impact of ransomware could be

evidenced from the worldwide “WannaCry” ransomware attack in May 2017. Discussing current cyber vulnerabilities, Mr Yeo explained that, with mobile and Internet-of-Things (IoT) devices being an integral part of our lives today, attacks on these devices were on the rise. He added that web-based attacks had decreased, while email-based attacks had increased, with one in every 131 emails being attacked. Mr Yeo also highlighted that there was a new strategy of stealth by hackers. He cited a hacker group known as “Strider”, which was stealthy enough to remain dormant in an organisation’s network, merging into the daily activities of the organisation and waiting for the time to attack.

Rear Admiral (Ret.) Janice M. Hamby
Chancellor, College of Information and Cyberspace, National Defense University
United States of America

Rear Admiral (Ret.) Janice Hamby began her presentation by pointing out that the term “cyber threat” was not appropriate. She argued that the threat was not a cyber-threat, but humans perpetrating attacks using cyberspace. Hence, she described cyberspace as a domain being leveraged to create a threat. She explained that the threat comes from criminals, terrorists, nation-states, and private sector competitors, while those being threatened are private citizens, corporate entities, nation-states, and the global network where commerce and diplomacy are being conducted. RADM Hamby elaborated that private citizens face threats such as ransomware, malware, and the lack of understanding of the technology, which causes them to make mistakes. The private sector, government services, and infrastructure face cyber threats such as denial-of-service attacks. Therefore, more work needs to be done to address these threats, she said.

At the international level, RADM Hamby suggested that a group of willing nations should come together to establish a set of norms for behaviour in cyberspace. For example, a group of willing nations could establish what constitutes acts of war in cyberspace and the specific roles within society and government. In addressing what the military could do, RADM Hamby emphasised that militaries need to understand cyberspace and the underpinnings of the network in order to develop a resilient strategy. Militaries must understand how tactical means in cyberspace could yield strategic effects, as well as individual responsibilities in observing safe practices on networks. Lastly, militaries need to be open to accepting their new and evolving role in cyberspace.

RADM Hamby expected that militaries would increasingly leverage cyberspace in their activities and that the key would be information. She noted that information had, in fact, become the seventh functional area for the US military. RADM suggested that it was important to understand the implications of using information to support or thwart the objectives of militaries and how the underpinning technology could enable that. She noted that the United States was also looking at resilience as opposed to robustness for developing deterrence in cyberspace. With resilience, militaries will develop the capability of "bouncing back" after cyber attackers have penetrated their systems. It is, after all, not realistic to focus on preventing cyberattacks, given the speed at which cyber criminals operate.

Question-and-Answer Session

The first question sought to ascertain how serious the problem of attributing attacks in cyberspace was. The questioner said some might argue that attribution was actually possible as governments were improving their capacity for identifying the source of cyberattacks. Also, as long as there was a demand for identifying the source of cyberattacks, the private sector would have the incentive to develop the capacity for attribution. Mr Yeo countered that it would be easy for adversaries to clean their trails in cyberspace and that a lot of data would be needed to accurately attribute an attack. Sometimes, one could discover that malware had already been embedded in one's systems years ago, and any response might be too late. RADM Hamby explained that since it would be extremely difficult to figure out the point of origin for attribution, she suggested that states look to international law for holding states and non-state actors accountable rather than focusing on attribution as an absolute.

The second question had five components: (i) what is Singapore's international standing in cybersecurity; (ii) what are the challenges that Singapore faces; (iii) how should Singapore overcome them; (iv) where does the balance lie between the use of technology and cybersecurity as Singapore becomes a tech-savvy nation; and (v) what are the different mechanisms that a military can leverage to reduce its threat exposure. Mr Yeo pointed out that Singapore's standing in cybersecurity was quite advanced in the Asia Pacific region. In terms of challenges to Singapore, Mr Yeo cautioned that there would be chaos in the adoption of technology if the implications were not well understood. RADM Hamby thought the biggest challenge facing Singapore would be one of culture. She believed the way Singapore uses information and how it uses technologies for sharing information must change. There must an appreciation that each individual was responsible for everyone else's information security apart from his or her own. Singapore should strike a balance between being bold in employing information and ensuring security for that information. Asst Prof Raska felt the SAF would need to be operationally adaptable and organisationally flexible. The SAF would need to think like its adversaries in order to counter the threat they posed.

The third question was related to whether cyber deterrence was achievable. Asst Prof Raska said that it was vital to understand that strategic conditions were changing with the advent of cyberspace. For instance, he argued, the cyber domain had levelled the playing field between weaker and stronger states. Cyber capabilities allowed weaker states to offset their

inferior conventional capabilities. The question then was how we should conceptualise cyber deterrence under such changing strategic conditions: should we use the traditional concept of deterrence or should we rethink the whole concept of deterrence. Mr Yeo suggested that cyber deterrence could only be achieved if there was better detection. He noted that we were often looking at best practices and ways of preventing cyber-attacks. However, best practices might not be sufficient as they might not apply to every organisation. What has been uncovered thus far is limited; and many cyberattacks remain undetected. Mr Yeo felt that many organisations lack this understanding.

The last question was centred on the disadvantages of having a single agency to address cyber threats. RADM Hamby said that having a single organisation to be responsible for cyber policies was akin to making the IT department of an organisation responsible for all cyber solutions. She argued that it made sense to have organisations functionally responsible for different aspects of cyberspace. For instance, the Cyber Command in the United States is responsible for the military's operations in cyberspace and the defence of the military network. But at the wider national level there needs to be a cross-functional view to get the strategic policies right. She noted that one problem of cyber deterrence was that many think of it as purely a cyber problem although there are other levers that could be pulled to help create a level of deterrence. The diplomatic community could be a part of creating a solid ground for deterring actions in cyberspace through sanctions and other diplomatic means, she suggested.

Panel 2: Confronting Cybersecurity Challenges

Mr Benjamin Ang
Senior Fellow, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

Mr Benjamin Ang began his presentation by giving an overview of the civilian cybersecurity strategy in Singapore that focuses on building a resilient Critical Information Infrastructure (CII) with 11 sectors, such as telecommunications, power, health, and finance. In his view, this constituted a robust framework to protect the critical sectors that provide essential services.

Mr Ang noted that a Cybersecurity Readiness Maturity Assessment exercise in 2012 had led to the implementation of a CII protection programme for government agencies and CII operators. The programme facilitates information exchange among CII operators. At the government level, cybersecurity "hygiene" standards have been implemented. A culture of cyber risk literacy is being developed to ensure awareness of the risks on the part of every individual. In addition, government services have been secured by a separation of the networks, which seemed to have been successful in warding off the last "WannaCry" attack.

Mr Ang went on to say that the government was now concentrating on creating a safer cyberspace for all. This, in his opinion, is a more challenging task as it will take more effort than the current action plan put in place for critical infrastructure. It would involve law enforcement aspects, which include educating the public, equipping the police, developing the tech-crime unit, reviewing the laws on hacking as well as partnering industry and overseas law enforcement.

Beyond fighting cybercrime, Mr Ang argued that each individual has a collective cyber responsibility. As the use of data networks becomes more prevalent and networks are decentralised, the government is unable to protect every single data network. With more everyday devices such as television sets having “smart” capability, there is a greater need for individuals to be cognisant of the risks that such connected devices present.

Another area of focus for Singapore would be to develop a vibrant cybersecurity ecosystem, continued Mr Ang. In this area, he said the Singapore government, with an eye on the expected growth in demand for cybersecurity, had provided funding and opportunities for working professionals to stay in the industry as well as for fresh graduates to enter it. This would, in turn, attract start-ups as well as encourage established companies in the industry to continue to base themselves in Singapore.

In the area of international partnerships, Mr Ang emphasised that the establishment of such partnerships as well as of cyber norms was especially important in this threat environment for small states like Singapore that depend on the rule of law for protection from bigger states. He noted that Singapore had established vital partnerships in recent years to combat cybercrime, with INTERPOL setting up a regional centre focusing on cyber threats in Singapore. There has also been increased cooperation within ASEAN, with a focus on security drills, in order to facilitate coordination among the member states.

Summing up, Mr Ang highlighted that additional legislation would be introduced in Singapore within the next few years after gathering inputs not only from government agencies but also from industry. This additional legislation would complement the existing laws that deal with unauthorised access into systems.

The Path Towards A Secure Cyberspace

Mr Lim Thian Chin
Deputy Director, Critical Information Infrastructure Protection Division, Cyber Security Agency
Singapore

Mr Lim Thian Chin started his presentation by noting that the Fourth Industrial Revolution was well under way, transforming every facet of our lives. Artificial Intelligence, big data and the Internet-of-Things (IoT) have significantly transformed the landscape and increased opportunities for all. However, at the same time, these same instruments have also made us vulnerable to cyberattacks as their use becomes more prevalent.

Mr Lim argued that while Singapore had been building up its capabilities to defend against cyberattacks, criminals and other adversaries were also evolving and developing innovative ways to circumvent and exploit the increasingly connected world. Ransomware and "WannaCry" attacks are no longer just social inconveniences but have the ability to put lives at risk by disrupting essential services at critical junctures. State-sponsored cyberattacks have also threatened state sovereignty and undermined trust in the digital future. Mr Lim said Singapore was not immune to such attacks; instead, it was more exposed than many other states owing to its "tech-savvy" society as well as the Singapore government's initiative to harness technology to improve the lives of Singaporeans.

Mr Lim argued that the digital economy was vital in ensuring Singapore's survival and that its push to be a "Smart Nation" played a critical role in this process. Major investments have been made to improve the digital economic infrastructure, and the Singapore government is leveraging IoT to bring

manufacturing to the next frontier, strengthening the country's position as a premier transshipment and logistics hub. However, Mr Lim warned that the more we embraced the digital economy, the more we would have to ensure that we were "cyber-secure."

As the Singapore government delivers more public services through digital platforms, Mr Lim said, the security of these platforms becomes a critical determinant of public trust. He said the Smart Nation sensor platform, which was designed to collect, analyse, and share data from sensors across the entire island, would help Singapore improve public services and serve Singaporeans better. Nevertheless, the public would reasonably expect that their personal data remains confidential under this data collection and that transactions are secure. If there are cyber breaches which compromise personal confidential information or undermine the critical data upon which the Singapore government decides policies, the public would lose trust in the government.

Mr Lim then highlighted a few challenges that Singapore would face in cybersecurity. First, cyber infrastructure and systems are constantly updated to guard against cyberattacks, only to find new viruses being developed. It is like a never-ending cycle. Second, the lack of geographical boundaries makes the nature of cyber-attacks different from traditional and conventional threats. Cyber threats could come from anywhere in the world. Third, a different understanding of distance, borders, and physical proximity in the cyber domain presents the problem of jurisdiction and law enforcement.

Summing up, Mr Lim said cybersecurity should not be seen as a threat to innovation. The aim of the Cyber Security Agency (CSA), he said, was to re-cast mental models and position cybersecurity as an enabler to leverage technology fully. This would, in turn, help Singapore to fulfil its vision of becoming a Smart Nation.

Defending Singapore in the Cyberspace

Colonel Teoh Chun Ping
Director (Policy), Defence Cyber Organisation
Singapore Armed Forces

Colonel (COL) Teoh Chun Ping's presentation was focused on cyber warfare. He quoted the Prussian strategist Carl von Clausewitz and the Chinese strategist Sun Tzu to explain why many states were turning to cyber warfare as a weapon of choice: Clausewitz had written that war was a continuation of politics by other means, intended to compel the opponent to accede to our will, while Sun Tzu had said that the key was to subdue the enemy without fighting. COL Teoh noted that cyber operations were being modified to resemble kinetic operations, with many defence companies and militaries modelling cyber operations on conventional kinetic operations.

COL Teoh likened the evolution of cyber power to that of conventional forms of warfare, notably airpower, which had evolved quickly from playing a mere support role in early warfare in the form of reconnaissance operations to a mainstream role in World War 2 and eventually to a standalone role, such as during the 1999 NATO air campaign in Kosovo. Cyber power, for its part, had evolved from being just a support tool to one that can replace kinetic operations, as evidenced by the Stuxnet worm attack on Iran's nuclear facility in 2010. COL Teoh argued that it was not inconceivable that war campaigns in future could be waged entirely in cyberspace. The capacity for cyberattacks is not limited to large states; small states are able to wage cyberattacks even without using their own capabilities. For example, the United Arab of Emirates (UAE) allegedly hired Russian hackers to launch an attack on the Al Jazeera television network during the Saudi-led siege of Qatar earlier in 2017. COL Teoh recalled that the personal data of Singapore's National Servicemen (NSF) and active military personnel had been compromised by a cyberattack. While no operational information was lost, it was a stark reminder of the need to be alert and ready for such attacks at all times. COL Teoh stressed that Singapore took cybersecurity seriously and there was a whole-of-government effort to tackle cyber issues.

Elaborating on the whole-of-government cybersecurity effort apart from the role played by the Cyber Security Agency (CSA), COL Teoh introduced GovTech, which oversees the cybersecurity of the government sector and the implementation of the Smart Nation concept. He also noted that the establishment of the Defence Cyber Organisation (DCO) underscores the critical importance of the cyber domain in military operations. The role of DCO is to lead and coordinate cybersecurity efforts across the entire defence cluster, which comprises SAF military networks, MINDEF/SAF corporate IT systems, the networks of the Defence Science and Technology Agency (DSTA) as well as the Defence Science Organisation (DSO). DCO also oversees the governance of the defence industry partners as well as MINDEF-related organisations.

Highlighting DCO's structure, COL Teoh noted that the organisation is comprised of three entities: (i) Cyber Security Division, an operational arm of DCO, which leads and coordinates the cyber defence of the entire defence cluster; (ii), Policies and Plans Directorate, which formulates the overall cyber defence capability development plan for the defence cluster; and (iii) Cyber Security Inspectorate, which conducts vulnerability assessment and penetration testing across the whole defence cluster. COL Teoh revealed that full-time NSF will also be recruited into the DCO via a stringent process. This would enable DCO to harness a wider pool of cyber talent and grow to a capacity of 2,600 staff in the next 10 years.

COL Teoh felt that the defence community could play a role in the whole-of-government effort to widen the country's pool of cyber talent. The defence community, through DSTA, organises an annual Cyber Defenders Awareness Discovery Camp, which is a three-day camp for about 400 tertiary students, who not only pick up programming and cybersecurity skills but also participate in cyber competitions. The best performers could be roped into DCO's pool of NSF cyber defenders.

At the ASEAN-level, COL Teoh cited the ASEAN Defence Ministers' Meeting Plus (ADMM-Plus) Expert Working Group (EWG) on Cyber Security as an important step towards fostering cyber defence cooperation among members of the regional grouping. He said Singapore will lend its full support to the co-chairs of the EWG, the Philippines, and New Zealand. Singapore will also be looking at ways of enhancing this cooperation during its own chairmanship of ADMM and ADMM-Plus in 2018, such as by affirming cyber norms and building regional communication in the event of a cyberattack.

In conclusion, COL Teoh warned that cyber threats would evolve both in terms of skill as well as complexity and there was a need to stay abreast of the threats. This would require not only a whole-of-government effort but also a whole-of-nation effort.

Question-and-Answer Session

Mr Ang was asked whether cyber hygiene needs to be taught from a young age and whether it was possible for older people to grasp its importance. Mr Ang replied that cyber hygiene had to be taught from a young age. He noted that CSA had been taking steps to educate school students. However, he stressed that it was not just the young who needed to be educated, but everyone in society. According to him, the real risks come from digital natives, who have grown up with technology and may be complacent when it comes to cybersecurity.

One participant asked whether there should be more emphasis on solving the attribution issue rather than simply adopting a defensive approach when it comes to cyberattacks. COL Teoh replied that identifying who was truly responsible was problematic. He elaborated that there were sometimes third parties who were interested in creating, and in turn benefiting from, conflict between two parties, and that wrongful attribution might lead to an escalation of the conflict. Mr Ang agreed that attributing an attack and taking offensive action might not be the best course of action, and, in some cases, might not even be effective against certain parties. He believed that at the policy level defence might be a more realistic form of deterrence.

Asked about the challenges of building cyber norms, Mr Ang said one should not just focus on the challenges, but also look for opportunities. The sheer number of states involved means that it would take time for all parties to agree on cyber norms. This would be especially the case for ASEAN, where decisions need to be reached by consensus. However, this also presents an opportunity to bring everyone to agree on a common framework, said Mr Ang.

Panel 3: Evolving Threat of Terrorism

Professor Rohan Gunaratna
Head of International Centre for Political Violence and Terrorism Research
S. Rajaratnam School of International Studies
Singapore

Professor Rohan Gunaratna's presentation was focused on the threat of the so-called Islamic State (IS) movement within the Indo-Pacific region. He said the Southeast Asian threat landscape was characterised by three interlinked developments that affect the security and stability of the region:

(i) The pledge of allegiance to IS leader Abu Bakr al-Baghdadi by several groups in Southeast Asia. These groups used to be independent or a part of the Al-Qaeda movement but have now become driven by IS ideology.
(ii) The development of an IS presence in the cyber domain. The IS presence has had significant impact on the ground by interfacing with and radicalising segments of the Muslim community in the region.
(iii) The expansion and decentralisation of IS-linked groups. While terror groups were traditionally created by locals, sent for training abroad, and returned to organise plots in their home countries, today, groups have increasingly started to plan from abroad, whether from Thailand, Indonesia, the Philippines, or even Syria.

Prof Gunaratna stressed that the most important element in protecting Singapore was securing the wider region, not just guarding Singapore's borders. He felt that the military played an important role in this process,

by working with and engaging other security actors in the region. As IS groups in the region are trans-boundary, he said the need for inter-regional cooperation is significant. For example, it was a Malaysian scholar who had created the regional command of IS, located in the Southern Philippines, and attacks throughout Southeast Asia were directed by this command. Prof Gunaratna also highlighted that the IS forces fighting in Marawi to help combat Philippine security forces came from throughout the region, that is, from Indonesia, Malaysia, and Singapore.

In conclusion, Prof Gunaratna stressed that any effective regional response to the IS threat would need to start by containing, then isolating, and finally eliminating the group.

Ambassador Mohammad Alami Musa
Singapore's Non-Residential Ambassador to Algeria
Head of Studies in Inter-Religious Relations in Plural Societies Programme
S. Rajaratnam School of International Studies
Singapore

Ambassador Alami Musa presented on the nexus between fundamentalism and violent extremism today. He explained that he wanted to counter the idea that violence was perpetrated only by the poor, down and out, and uneducated masses. Rather, there is growing evidence that wealthy and highly educated people join terrorist groups. Indeed, the largest delegations of foreign fighters in Syria came from Algeria and Tunisia. Most of them were from well-to-do families. Ambassador Alami posited that fundamentalism was a creation of modernity. Modernity freed the European man from the dominant Church as well as from tyranny and suppression. This social revolution in turn brought about a huge growth in difference and diversity.

With the explosion of ideas and views, truth and reason were no longer certain. As such, there was a heightened sense of anxiety, uncertainty, and fear.

Ambassador Alami explained that this uncertainty and fear led men to beliefs and ideologies that provided certainty, such as fundamentalism, which was not based on universal reason nor could be tested against the truth. He elaborated that this dynamic was intensified when combined with secularism. In the post-colonial era, Muslim-majority states became independent and secular states, but what it meant to be living in a secular state or society was not impressed on the people. Faced with corruption and mismanagement that fed resentment and backwardness, the people became resentful and increasingly hostile towards the West and the faiths of others. Thus emerged fundamentalists, who sought to find verses in the Qur'an and the other sacred texts that could be interpreted to support their extremist actions.

Mr Michael Miklaucic
Director of Research; PRISM Editor
Center for Complex Operations, National Defense University
United States of America

The focus of Mr Michael Miklaucic's presentation was on the convergence between extremist and criminal groups. Mr Miklaucic first debunked President Donald Trump's notion that there was a need for a war against radical Islamic extremism and President George W. Bush's declaration 16 years earlier of a war against terrorism. He contended instead that the real war was for the preservation of the global order of accepted rules that governed the behaviour between states. He also emphasised that the challenge was not localised to the Middle East nor was it strictly a terrorism issue. He said there was the mistaken assumption that terrorists would not want to be tarnished by association with criminal gangs as they were driven

by political or ideological grievances, unlike the latter. Criminals, too, were thought to be avoiding association with terrorists to prevent being targeted by special forces. Mr Miklaucic argued that these distinctions between terrorists and criminals had outlived their utility in a world where the two elements collaborate, collude, and cooperate. The world had been mistakenly treating them as separate phenomena and fighting them separately.

Mr Miklaucic stressed the hybrid nature of modern terrorist and criminal groups. He used the example of the Lebanese group Hezbollah, which once was a pure terrorist group but has since branched out into smuggling drugs, gold, and cigarettes. In an increasingly networked world, the connectivity between these two types of groups has increased, bringing about a convergence between terrorists and criminals. The threat comes when massive amounts of money gained through criminal activities are used to finance larger and more influential terrorist groups. Mr Miklaucic contended that this convergence was creating an alternative global economy that challenges the global order of sovereign states. The greater concern, thus, should be the gradual corrosion of the global order that began in Westphalia in 1648.

Question-and-Answer Session

The first question was centred on how militaries could help combat terrorism. Mr Miklaucic argued that the military has a fundamental role but this could vary, depending on individual states. He stressed the need for the military to collaborate with law enforcement and intelligence agencies. He singled out three distinct areas where the military could support the counterterrorism effort: (i) information sharing since the military usually had unique gathering capabilities; (ii) bringing in heavier firepower where threats go beyond the ability of law enforcement to address; and (iii) drilling and exercising according to specific threat scenarios. Mr Miklaucic pointed out that many agencies assumed they could work together if forced to, but, in reality, they struggled to do so. Without preparing and exercising, different agencies would find that communication channels were not working or that their respective rules of engagement were dissimilar. The key to success is to identify these gaps early on, rather than during a crisis. Prof Gunaratna argued that there was a gap in the capabilities of the military, law enforcement, and other security agencies. He observed that there was such a gap even in Singapore, albeit not as significant as that in other states. The threat of terrorism, he said, was so overwhelming that the military would have to play a proactive role and not just a reactive one. He cited the example of Indonesia, where the military and police were cooperating through joint training and operations. He warned that unless the military worked closely with law enforcement and intelligence agencies, the threats would grow rapidly.

The next questioner wanted to know whether the trend in terror attacks was towards major and dramatic attacks or smaller-scale ones. Prof Gunaratna believed that most IS attacks would continue to be smaller, lone wolf attacks, rather than large-scale ones. However, he stressed that large-scale attacks remained a threat and were actively being planned by terrorist groups. Mr Miklaucic agreed but noted that it would not be just a threat from Islamist radical groups but also other terrorist groups, such as the Aum Shinrikyo in Japan. Aum Shinrikyo attacked the Tokyo subway station with sarin gas in 1995, but because of its lack of understanding of air-conditioning only 12 people died. If the group had been better informed, there might have been thousands of casualties. Mr Miklaucic argued that there was a need to anticipate the unexpected and to imagine the unimaginable.

Another participant asked Mr Miklaucic for his views on how to educate officers to deal with ideological and other future issues facing the military. Mr Miklaucic stated that there was a need to systematically steer faculty

members trained in traditional military studies towards focusing on non-traditional and emerging security threats. He also argued that there was a need to rethink the division of issues into military and non-military ones. Mr Miklaucic felt that such a division tended to handicap governments as enemies do not observe them. He pointed out that there was an ongoing effort to update the American curriculum to make it more relevant to current realities.

The final question, directed to Ambassador Alami, sought to probe why a young Singaporean Muslim would be motivated to join IS despite the Singaporean Muslim identity being highly tolerant. Ambassador Alami, who is also president of the Islamic Religious Council of Singapore or MUIS, answered by sharing his experience in shaping the Singaporean Muslim identity. He said that after the September 11 attacks, there was deep concern that the Singaporean Muslim community would start identifying with the global ummah (Muslim community). Had that happened, the directions, guidance, and inspiration would have come not from Singapore but from the global centre of Islam in the Middle East. Faced with this ideological threat, MUIS focused on how to contextualise and localise Islam. Ambassador Alami said a unique identity for Singaporean Muslims had subsequently been forged. However, he lamented that there were exceptions to the norm and that it was not always possible to reach out to everybody.

Panel 4: Countering the Threat of Terrorism — Strategies and Approaches

Countering Terrorism in Singapore

Dr Norman Vasu
Deputy Head, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

Dr Norman Vasu began by discussing what he saw as the distinction between countering terrorists and countering terrorism. The countering terrorist aspect, in his view, was about a kinetic approach to the problem while countering terrorism was about creating a negative operating environment for terrorists where they would not be able to get a support base among the populace.

Dr Vasu highlighted the four common steps that most states would attempt to take in countering terrorism. First, most states would try to disprove the master narrative of the terrorists and offer a counter-narrative. Terrorist organisations, he noted, were good at providing values and a sense of purpose. As such, the role of the state is to provide a different sense of purpose for society so that the population would not be attracted to the fundamentalist ideology.

Second, Dr Vasu said most states would want to attend to popular grievances. Most populations would want development and not disenfranchisement. If the state is not successful in improving the socio-economic conditions of local communities, the latter may fall into the trap of the fundamentalists' propaganda, which is in part to convince the population that their socio-economic needs would be better met by the fundamentalists.

Third, Dr Vasu observed that, in their outreach programmes, most states might be able to reach out to those groups that might not be attracted to fundamentalist ideology but they often tended to misunderstand those people who were likely to fall sway to such ideologies. Hence, there is a need for outreach programmes to demystify the "other". The rationale behind this approach is to develop social bonds so that the terrorists' master narrative would lose some of its traction.

Fourth, Dr Vasu talked about the need for states to place greater emphasis on inter-religious dialogue. He argued that inter-religious dialogue was meant to humanise people who hold beliefs different from one's own. The aim is to create greater awareness of commonality than of differences. With stronger social bonds, society would have better resilience and this in turn would help overcome problems quite quickly.

Moving on to Singapore's approach, Dr Vasu argued that the government had been engaging in counterterrorism long before September 11 without being aware of it. Since independence, the Singapore government had always been attempting to create social bonds. Dr Vasu highlighted Singapore's principles of meritocracy and multiculturalism, which laid the ground rules for the development of social bonds. Singapore, being a multi-cultural society, no one community is preferred over the other. This principle of multiculturalism is supplemented by the practice of meritocracy, where hard work is recognised.

Dr Vasu noted that after September 11 the Singapore government increased the level of counterterrorism work by forming Inter-Racial and Religious Confidence Circles (IRCCs). The IRCCs are community engagement programmes that reach out to different spheres of Singaporean society. The Singapore government had also introduced the "SGSecure" initiative, with its three pillars of staying alert, united, and strong. Dr Vasu noted that the middle pillar was about building social bonds, which is a continuation of what had been done before.

In closing, Dr Vasu argued that the Singapore government had not been very good at articulating a strong sense of purpose as part of offering a counter-narrative to the narrative that fundamentalists put out. The sense of purpose it had articulated was centred on unity and prosperity but Dr Vasu said this was rather vague. In order to effectively counter terrorism, Singapore had to counter the fundamentalist ideology strongly. Thus, Dr Vasu felt that the Singapore government ought to think about creating a stronger sense of purpose in Singapore.

Regaining the Initiative: Terrorist Learning and Red Teaming – A Student's Perspective

Major Benson Chian
Student, Goh Keng Swee Command and Staff College (GKS CSC)
Singapore Armed Forces

Major Benson Chian began by discussing the terrorist threats that Singapore faces, given its unique conditions and inherent vulnerabilities. Singapore, he noted, was a lucrative target for terrorists as it was friendly to Western economic and commercial interests. The Singapore government had also regularly spoken out and acted against terrorists. Being a multi-racial society, perpetrators could potentially exploit and provoke polarisation in Singaporean society, said MAJ Chian. The proliferation of new media has also allowed opportunities for some Singaporeans to access extremist propaganda and become radicalised over time. In addition, Singapore's high dependence on a non-resident labour force represented a risk. These non-residents of foreign origin might be potential proxies for adversaries to leverage for strikes against Singapore.

MAJ Chian then moved on to talk about the approaches that terrorists adopt in learning and in evolving their plans. Terrorists, he said, use self-learning and are able to adapt and innovate their learnings. There is also transfer of such learnings within, and between similar, groups. Propaganda magazines and illicit materials that are easily available online are the main sources for self-learning. Terrorist organisations have also demonstrated that they can adapt and innovate. For example, in order to overcome surveillance

by intelligence agencies, jihadist cells have become more autonomous and switched their weapon of choice from explosives to close up weapons. This change was observed in the murder of British soldier Lee Rigby on the open streets of London in 2013. Overall, understanding how terrorists learn can strengthen early detection and response to their attacks.

MAJ Chian then proposed a red teaming strategy, which would enable security agencies to stay ahead of terrorists. He contended that red teaming, a strategy whereby teams assume the role of the adversary and think like them, provides a means of identifying our vulnerabilities ourselves before terrorists do. Terrorists are constantly changing their concept of operations to outsmart security agencies, so we need a more proactive approach to complement our current strategies, he said.

MAJ Chian suggested that one key enabler of red teaming is harnessing data by crowd sourcing. He argued that red teams could leverage the whole of society to identify and report previously unknown vulnerabilities. Red teams could then focus on examining these vulnerabilities through robust risk assessment matrices and prioritise action against them based on their impact. All data would need to be considered to avoid missing small but nevertheless important pieces of information. In managing big data, data fusion and analytics could enable the extraction and grouping of large volumes of data.

In conclusion, MAJ Chian argued that the evolving threats require that Singapore enhance its counterterrorism strategy by using red teaming to regain the initiative from terrorists.

Professional Military Education's Approaches in Educating Senior Officers on Global Terrorism

Professor Andrea Dew
Co-Director, Center for Irregular Warfare and Armed Groups (CIWAG),
US Naval War College
United States of America

Professor Andrea Dew began by describing two ways of thinking about the complexity of cyber and terrorist challenges: thinking in a focused orbit and coming out with a programmed response or choosing to be exposed to different ideas and deriving different solutions. Prof Dew suggested that military leaders should strike a balance between these two types of thinking. They need to be extremely good at the focused part because soldiers would be relying on them for quick decisions. At the same time, they must be thought leaders who are not simply rote thinkers.

Addressing the benefit of red teaming, Prof Dew said that one seam and gap in counterterrorism lay in the fact that agencies tend to draw lines to delineate responsibilities. Our adversaries could exploit this seam and gap. She raised the analogy of a simple neighbourhood riot where resilience could be destroyed in its aftermath. The riot could do very little damage in terms of destroying buildings but it could do an extreme amount of damage in destroying relationships. There could be no plan for building back relationships because neighbourhood leaders draw lines between each other and never get along well. Our adversaries know that if they pressed on this

seam, they could do far more destruction. Red teaming is about identifying these seams and gaps.

Prof Dew drew attention to both institutional and legal seams and gaps. As an example of the former, she cited ASEAN, where a determined adversary could pick at the weaker member states. If there was enough pressure, it could affect the entire organisation. Prof Dew then used the example of the Mumbai attacks of 2008 to illustrate legal seams and gaps. The Mumbai attackers came from sea and it was the responsibility of the navy to stop them. However, the Indian navy looked at the trawler that the men were on and concluded that it did not figure in its list of concerns. As the attackers came close to shore, the coastguard allowed them to pass because they were not considered smugglers. Hence, there was a jurisdictional problem that allowed the Mumbai attacks to take place.

Citing a statement by Osama bin Laden in 2004, Prof Dew noted that the terror leader had identified America's seams and gaps to lie in protraction and attrition. Osama felt that if he could protract the conflict, he could exhaust the Americans by exploiting their unwillingness to take casualties and stay in the fight. Although the Americans are still in the fight, it was good thinking on the part of Osama at that point of time, Prof Dew commented.

In her concluding remarks, Prof Dew said that beyond just identifying their own seams and gaps, states should also poke at their adversaries' seams and gaps. Doing so would help them gain a competitive advantage over terrorists, short of kinetic operations.

Question-and-Answer Session

On the issue of addressing public grievances, one participant noted that some grievances could not be addressed. For example, with the salafi jihadists (Islamist puritans who believe that armed warfare is an individual obligation), who tend to take a black and white world view, there are grievances that can never be addressed without putting ourselves out of existence. Dr Vasu agreed and said it would be a lot easier to address individuals with a liberal bent of mind as they would tend to think of grievances in the material sense. Dr Vasu believed individuals with an extreme ideological mindset represent a small fraction of humanity. However, he contended that even among the extremists there was some heterogeneity and there could well be individuals that we could speak to.

The next question was a broad one relating to the ideological problem that cannot be tackled by the military alone. The questioner wondered how the military might play a constructive role to help the state respond to terrorist organisations. Prof Dew responded by using the example of the United States, where society is polarised between two ideological camps. US Secretary of Defense James Mattis, she said, had once mentioned that the job of the military was to be apolitical and to ”hold the line”. Dr Vasu felt that the military was good at giving a sense of purpose. In the Singaporean context, National Service was an interesting experiment to see whether Singapore could create a nation by getting all males to be part of a mission, he said.

The last question was on Marcus Hansen’s “Third Generation Return” hypothesis, which posits that third generation immigrants typically return to traditional values. The question was how Singapore could reconcile ideological differences, especially for third generation citizens. Dr Vasu responded that Hansen’s view remains a hypothesis and has not been proven. In Singapore’s case, Dr Vasu said there are not many such third generation citizens yet. As for ideological differences, Dr Vasu said we should not think of ideology as a tactic where there could be a game plan that we could stick to in countering it. Ideology is constantly evolving and any plans to counter it could be challenged. Nevertheless, Dr Vasu felt that there should still be constant discussion of ideology.

Plenary Presentations

Participants broke up for three different group discussions after the four panels. The following is a summary of the groups' presentations during the plenary session.

The first group presented on the challenges that Singapore faces in implementing a comprehensive and cyber-secure environment. The group classified the challenges under the rubric of technical, definitional, organisational, and cultural. On technical challenges, the group felt the supply of cyber talent in Singapore was insufficient. By cyber talent, they meant individuals who could understand cyber systems, their vulnerabilities, and possibilities, and were, therefore, able to direct resources to outwit hackers. The group noted that there were different understandings of what constitutes a cyber-threat and what could be considered an act of war. This lack of agreement could bring about organisational challenges, where there is uncertainty whether to classify a cyber-threat as a military threat or a civilian-criminal issue. In turn, there would be no clarity on whether the response should be military-led or civilian-led. Given that the cyber domain has many different stakeholders, this could be an issue. On cultural challenges, the group noted that not many Singaporeans appreciate the complexity of cyber threats and see the need for cybersecurity.

The second group presented on how the Fourth Industrial Revolution complicates the cyber defence of Singapore, in both the military and wider

civilian domains. The group first discussed the complications for the military. Cyberspace constitutes a virtual domain that the SAF is not used to. This is compounded by the advent of Artificial Intelligence (AI), which is a key feature of the Fourth Industrial Revolution. AI has the possibility of creating a man-out-of-the-loop situation. Today, decision-making is still left to humans, but this may not be true in the future. The military will then be no longer pitted against humans but against software that can actually launch a weapon. In such an instance, there can be plausible deniability by states and non-state actors. This can complicate the military's response. At the national level, as Singapore gets more connected in the virtual world, it is exposed to the risk of amateurs downloading from the cloud software with advanced capabilities.

The third group considered whether terrorism is limited to asymmetric conflict and whether terror can be used to complement conventional attacks. The group defined terrorism as an act of violence designed to incite fear and achieve political objectives. They argued that terrorism is inherently asymmetrical as it allows the weaker party to counter a stronger party. At the same time, terrorism is increasingly being used by perceived stronger parties. In a practical sense, terrorism can be used as a force-multiplier in conventional operations. The group cited examples of state-sponsored terrorism, where countries use terrorism when they do not want to get their hands dirty.

The fourth group presented on the challenges of counterterrorism in the Asia-Pacific region and the practical ways that militaries of the region can cooperate with one other. The group argued that what constitutes a terror act for one state may not be viewed in the same way by another state. This could pose a challenge to effective cooperation in counterterrorism. The group contended that another challenge lies in the sharing of intelligence. States might not share intelligence if they thought such sharing could affect their national interests. Separately, the group highlighted the issue of competence among the different counterterrorism forces in the region. If more countries were involved in counterterrorism, the challenge would be to manage the vast disparity in competence. The group proposed that militaries could make use of defence diplomacy platforms to facilitate an exchange of ideas. One such platform could be the ASEAN Defence Ministers' Meetings Plus (ADMM-Plus).

Closing Remarks

In summarising the key points that emerged during the seminar, Colonel (COL) Simon Lee Wee Chek made the following comments:

(i) Terrorist organisations such as IS are constantly innovating in terms of military technology. The SAF has recognised that the military technology syllabus needs constant updating and reinventing so as to generate greater appreciation of military technology, just as how IS appreciates innovation.

(ii) In a total war scenario, perpetrators do not respect the distinction between peacetime and wartime. Thus, the military needs to break out of its stovepipe and understand that the exposure to cyber and terrorist threats takes place every day. In this regard, cyber and terrorist threats call for the highest level of defence readiness, or DEFCON One, every day. The challenge lies in balancing the military's resources.

(iii) Counterterrorism is a whole-of-government and whole-of-nation effort. In this regard, Singapore has made a significant breakthrough in eliminating the boundaries between MINDEF, SAF, the Ministry of Home Affairs, and the Police Force. However, regional cooperation on counterterrorism is somewhat limited owing to conceptual differences.

Overall, COL Lee felt that the seminar had done well in providing a platform for the GKS CSC and the SAF to take a deep dive into the complex issues of cyber and terrorist threats.

Seminar Programme

Day 1: Thursday, 5 October 2017

0900 hrs **Opening Remarks**
Colonel Simon Lee Wee Chek
Commandant, Goh Keng Swee Command and Staff College
SAFTI Military Institute
Singapore Armed Forces

0910 hrs **Keynote Address**
Mr Ng Chee Kern
Permanent Secretary (Smart Nation and Digital Government)
Prime Minister's Office, Singapore

1000 hrs **Coffee Break**

1030 hrs **Panel 1: Emerging Issues, Trends, and Implications of Cyber Threats**

Speakers
Assistant Professor Michael Raska
Military Transformation Programme
Institute of Defence and Strategic Studies (IDSS)
S Rajaratnam School of International Studies (RSIS)
Singapore

Mr Matthias Yeo
Chief Technology Officer (APAC), Symantec Corporation
Singapore

Rear Admiral Janice M. Hamby
Chancellor, College of Information and Cyberspace, National Defense University
United States

Chair
Professor Pascal Vennesson
Professor of Political Science, IDSS, RSIS
Singapore

1200 hrs **Lunch**

1300 hrs **Panel 2: Confronting Cybersecurity Challenges**

Speakers
Mr Benjamin Ang
Senior Fellow, Centre of Excellence for National Security (CENS), RSIS
Singapore

Mr Lim Thian Chin
Deputy Director, Critical Information Infrastructure Protection Division, CSA
Singapore

Colonel Teoh Chun Ping
Director (Policy), Defence Cyber Organisation
Singapore Armed Forces

Chair
Assistant Professor Ong Wei Chong
Assistant Professor, Military Studies Programme, IDSS, RSIS
Singapore

1430 hrs **Coffee Break**

1500 hrs **Syndicate Discussions**

❖❖❖

Day 2: Friday, 6 October 2017

0900 hrs **Panel 3: Evolving Threat of Terrorism**

Speakers
Professor Rohan Gunaratna
Head of International Centre for Political Violence and Terrorism Research, RSIS
Singapore

Ambassador Mohammad Alami Musa
Singapore's Non-Residential Ambassador to Algeria, and
Head of Studies in Inter-Religious Relations in Plural Societies Programme, RSIS
Singapore

Mr Michael Miklaucic
Director of Research, PRISM Editor, Center for Complex Operations
National Defense University
United States

Chair
Mr Eddie Lim
Head of Military Studies Programme, IDSS, RSIS
Singapore

1030 hrs **Coffee Break**

1100 hrs **Panel 4: Countering the Threat of Terrorism – Strategies and Approaches**

Speakers
Dr Norman Vasu
Deputy Head of the Centre of Excellence for National Security (CENS), RSIS
Singapore

Major Benson Chian
Student, Goh Keng Swee Command and Staff College (GKS CSC)
Singapore Armed Forces

Professor Andrea Dew
Co-Director, Center for Irregular Warfare and Armed Groups (CIWAG)
US Naval War College
United States

Chair
Associate Professor Ahmed Hashim
Military Studies Programme, IDSS, RSIS
Singapore

1230 hrs **Lunch**

1330 hrs **Syndicate Discussion**

1500 hrs **Coffee Break**

1530 hrs **Plenary Presentation**

Chair
Mr Eddie Lim
Head of the Military Studies Programme, IDSS, RSIS
Singapore

1645 hrs **Closing Remarks**
Colonel Simon Lee Wee Chek
Commandant, Goh Keng Swee Command and Staff College
SAFTI Military Institute
Singapore Armed Forces

❖❖❖

List of Speakers

Assistant Professor Michael Raska
Assistant Professor
Military Transformations Programme
Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

Mr Matthias Yeo
Chief Technology Officer (APAC)
Symantec Corporation
Singapore

Rear Admiral Janice M. Hamby
Chancellor
College of Information and Cyberspace
National Defense University
United States of America

Mr Benjamin Ang
Senior Fellow
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

Mr Lim Thian Chin
Deputy Director
Critical Information Infrastructure Protection Division
Cyber Security Agency
Singapore

Colonel Teoh Chun Ping
Director (Policy)
Defence Cyber Organisation
Singapore Armed Forces

Professor Rohan Gunaratna
Head of International Centre for Political Violence and Terrorism Research
S. Rajaratnam School of International Studies
Singapore

Ambassador Mohammad Alami Musa
Singapore's Non-Residential Ambassador to Algeria;
President of Majlis Ugama Islam Singapura (MUIS); and
Head of Studies in Inter-Religious Relations in Plural Societies Programme
S. Rajaratnam School of International Studies
Singapore

Mr Michael Miklaucic
Director of Research, PRISM Editor
Center for Complex Operations
National Defense University
United States of America

Dr Norman Vasu
Deputy Head of the Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

Professor Andrea Dew
Co-Director
Center for Irregular Warfare and Armed Groups (CIWAG)
US Naval War College
United States of America

List of Chairpersons

Professor Pascal Vennesson
Professor of Political Science
Military Studies Programme
Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

Assistant Professor Ong Wei Chong
Assistant Professor
Military Studies Programme
Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

Mr Eddie Lim
Senior Fellow
Head of Military Studies Programme
Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

Associate Professor Ahmed Hashim
Associate Professor
Military Studies Programme
Institute of Defence and Strategic Studies
S. Rajaratnam School of International Studies
Singapore

About the Goh Keng Swee Command and Staff College

The Goh Keng Swee Command and Staff College (GKS CSC) is the Singapore Armed Forces' premier educational institution. All SAF leaders pass through the portals of GKS CSC.

Each year, specially selected officers attend the various courses offered at GKS CSC. Through the GKS CSC's course curriculum and extra-curricular activities, these officers acquire the requisite exposure to the complexities and challenges of leading the SAF into the future.

GKS CSC is proud to be one of three schools within SAFTI Military Institute, the other two being the Officer Cadet School (OCS) and the SAF Advanced Schools (SAS). Together, these schools provide holistic officer education and training for regular and National Service Full-Time officers of the Singapore Armed Forces.

About the SAF-NTU Academy

The SAF-NTU Academy's mission is to create and sustain the academic capacity and knowledge needed to equip military leaders with professional military knowledge using multidisciplinary approaches. The programme managed by SNA will contribute to the SAF's overall nurturing and engagement efforts to develop competent and committed military professionals. SNA is also charged with growing a pool of deep specialists skilled in both military and academic disciplines.

SNA oversees the SAF-NTU Continuing Education (CE) Master's and the SAF-NTU Undergraduate Professional Military Education and Training (UGPMET) programmes. SNA works closely with the SAF Education Office and Goh Keng Swee Command and Staff College at the SAFTI Military Institute and SAF Personnel Management Centres in the execution of its programmes.

Other than delivering education, SNA manages research, scholarship and collaboration programmes to ensure the renewal, creation and management of knowledge for educational purposes, and to raise the professional and academic standing of both the SAF and NTU.

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.