CENS – GFF Cybersecurity Workshop

The Geostrategic Implications of Cyberspace

18 – 19 July 2011, Singapore

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

NATIONAL SECURITY COORDINATION SECRETARIAT

GLOBAL FUTURES FORUM
CREATING NETWORKING POSSIBILITIES

CENS – GFF CYBERSECURITY WORKSHOP: THE GEOSTRATEGIC IMPLICATIONS OF CYBERSPACE

REPORT ON THE WORKSHOP JOINTLY ORGANISED BY
THE CENTRE OF EXCELLENCE FOR NATIONAL SECURITY (SINGAPORE)
AND
THE GLOBAL FUTURES FORUM (INTERNATIONAL)

WITH THE SUPPORT OF
THE NATIONAL SECURITY COORDINATION SECRETARIAT (SINGAPORE)

18–19 JULY 2011
MARINA MANDARIN HOTEL
SINGAPORE

CONTENTS PAGE

Rapporteurs: Wendy Chan, Damien Cheong, Yolanda Chin, Sulastri Osman, Jenna Park, Muhammad Saiful Adli Ayob, Yeap Suyin, Senol Yilmaz
Edited by: Jenna Park

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

The conference adheres to a variation of the Chatham House rules. Accordingly, beyond the points expressed in the prepared papers, no attributions have been included in this conference report.

EXECUTIVE SUMMARY

The Cybersecurity Workshop was held on 18-19 July 2011 at the Marina Mandarin Hotel under the theme "The Geostrategic Implications of Cyberspace". This marked the second year of cybersecurity workshop jointly organised by the Centre of Excellence for National Security (CENS) and Global Futures Forum (GFF) with the support of National Security Coordination Secretariat. The first cybersecurity workshop was held under the theme "Towards a Secure and Resilient Cyberspace" and the discussions revolved around the subject of cyber crimes which include terrorist attacks in cyberspace, financial fraud, and dissemination of propaganda and looked for ways to develop resilience and security in cyberspace in the face of its borderless nature. This year's Cybersecurity Workshop was a continuation of this discussion. Cybersecurity has constantly developed into a critical issue for both governments and private sectors in many countries the world over. Currently, the subject of cybersecurity is now not merely confined to technological and operational issues but even encompasses other critical national/international issues such as economy, politics, and legislation. In light of this, the second Cybersecurity Workshop was held to explore the current dynamics of cyberspace in these diverse aspects, its potential threats in the future, and policy options to address them from an international perspective in particular.

The two-day workshop consisted of a keynote address and five panels which comprised speakers with expertise from diverse backgrounds. In his keynote speech, Sean Kanuck shared the key analytic frameworks regarding threats, values, norms and risk of cybersecurity; he opined that it is crucial to maintain collective safety and welfare in cyberspace given the rapid technological advance. Panel 1 discussed the current situation of cyberspace, what its available capabilities were, and which actors or organisations had the capacity to regulate it. Panel 2 discussed how the cyberspace is being exploited as means of organised crimes by hackers as well as terrorist organisations, the magnitude of the problem and its trends, and how they could be dealt with. Panel 3 addressed the question of how nations view cyberspace in the context of projecting national power, who the main players were, and the capabilities currently being developed. This also involved the discussion of the legal, international, and diplomatic framework in the context of cyber conflict. Panel 4 looked into how ubiquitous networks and social networking tools in cyberspace affect public and strategic communications by organisations and nations, their social and political effects, and how they could be translated into national and international objectives. Lastly, Panel 5 comprised prominent personalities who spoke on the overall issue of cybersecurity from their own countries' perspectives. As the last session of the workshop, this panel was dedicated for open discussion between panellists and participants and saw active exchanges on the points raised during all the workshop sessions.

Overall, the discussions centred on the issue of attribution in cyberspace, the rapidity of technological advance and the necessity of constantly improving commensurate cybersecurity measures, vulnerability derived from the total reliance of all infrastructures on cyber networks, and the transnational character of cyberspace and its attendant complexities. As cyberspace is becoming a more challenging field in terms of national/international security, there was general agreement that the discussion must continue and address the evolving trends and threats in cyberspace.

WELCOME REMARKS BY CUNG VU

(Left to Right) Ruth David and Cung Vu

Cung Vu from the National Maritime Intelligence Centre and the Global Futures Forum (GFF) of the Department of State, welcomed speakers and participants to the Cybersecurity Workshop, jointly organised by the Centre of Excellence for National Security (CENS) of the S. Rajaratnam School of International Studies (RSIS) and the GFF, with the support of Singapore's National Security Coordination Secretariat (NSCS) under the Prime Minister's Office.

Citing the recent attack on Sony Corporation's network, which had cost the company damage of USD 173 million, Vu noted that within a year of the CENS-GFF Cybersecurity Workshop being held in 2010, cyber attacks were still constantly on the rise. Moreover, one no longer needed to be a professional hacker to hack into networks. For example, customisable hacking codes provided by such hackers allow non-hackers to easily hack into bank accounts among other things.

Cyber attacks are directed at nearly every sector of infrastructure and economy, and affect more than just the commercial sector. For example, in 2008 a foreign intelligence agency penetrated the classified computer systems in the US. To illustrate how the cyber threat today is far more serious than the 2008 attack, Vu highlighted the recent attack on a US defence contractor that allowed a group of foreign hackers to steal 24 thousand files which included blueprints of aircraft avionics, surveillance technologies, satellite communication and network security protocols.

Vu shared that in response to the threat of cyber attacks, the US Department of Defense (DoD) has released their strategy for operating in cyberspace. The five strategic initiatives included: i) treat cyberspace as an operational domain to organise, train, and equip so that DoD can take full advantage of cyberspace's potential; ii) employ new defence operating concepts to protect DoD networks and systems; iii) partner with other US government departments, agencies and the private sectors to enable a whole-of-government cybersecurity strategy; iv) build robust relationships with US allies and international partners to strengthen collective cybersecurity; and v) leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

WELCOME REMARKS BY BILVEER SINGH

In his welcome remarks, **Bilveer Singh**, Acting Head of CENS in RSIS, highlighted that the workshop marked the fourth year of collaboration between CENS, GFF, and NSCS. He stressed that cybersecurity continues to be very topical in light of the large-scale hackings of public and private sector entities and domains.

Singh stated that there were two distinct groups of hackers: non-state actors and state actors. Non-state actors include common criminals, terrorists, and "hacktivists" who engage in the non-violent use of illegal or legally ambiguous digital tools in pursuit of political ends. Some "hacktivists" use their technical knowledge for vandalism or protest. Notorious groups such as LulzSec and Anonymous have stolen and leaked classified information from governments, banks, and other high-ranking establishments.

The second source of cyber threats, Singh said, emanated from state-centric actors. These state actors are keen to obtain insights into other countries' political and strategic plans, research and development, as well as manufacturing know-how, or to hack into essential national infrastructure systems, possibly for military exploitation.

Singh observed that attribution is a major issue in the context of cybersecurity: hackers can conceal their identity or re-route their attacks, making it seem as though the attacks originated from different countries. Given the difficulty of identifying the intruders of computer systems, it is not always clear whether a state actor is behind such intrusions.

Nevertheless, experts surmised that the biggest threat to governments will come from other governments, as only state actors appear to have the discipline, commitment, and resources to develop capabilities to cause significant harm. One consequence of this type of state-sponsored cyber threat was Pentagon's recent announcement that it would treat cyberspace as the fifth operational domain of the armed forces – equal to land, air, sea, and space – and would invest huge sums in active cyber defence and encryption technologies.

In sum, Singh remarked that we may be entering the realm of a new form of non-conventional cyber warfare and counter-warfare. He noted that cyberspace has become increasingly securitised, warning that it might soon be militarised under current circumstances.

KEYNOTE SPEECH:

CYBERSECURITY FRAMEWORKS

Giving his keynote speech, **Sean Kanuck** outlined the key analytic frameworks regarding threats, values, norms and risks of cybersecurity. This was to enable the international community to reconsider what security means in the 21st century and more particularly, what security means in cyberspace.

According to Kanuck, the term "security" had two connotations. The first was a negative concept which involves the prevention of being harmed and can be equated with the notion of safety. The second connotation was a positive concept which involves promoting a better quality of life and protecting human rights, which can be associated with welfare. He proposed that a successful model of cybersecurity must entail welfare besides merely ensuring safety of cyber networks.

The current environment in cyberspace is complex and ever-changing. As Kanuck explained, the compounding rate of transformation brought on by information and communication technologies is altering social interaction, commerce, politics, and even warfare. The convergence of myriad networks, devices and protocols into a worldwide interoperable information system will certainly bring about irreversible results.

Kanuck stressed that any discussion on the enforcement of norms, deterrence of adversaries in cyberspace and prevention of cyber espionage or cyber attacks must also consider other legitimate competing norms. Policy makers from every country must balance sovereignty versus individual rights, such as the freedom of political speech. Moreover, they must understand that technological standards may expand or constrain the range of possible norms which could actually be implemented.

In order to operate effectively in cyberspace, Kanuck argued for the need to adopt a risk management model. He said that the more one develops risk models, the more one would be able to better appreciate why cybersecurity is such a difficult problem. He added that most threats with global reach have identifiable footprints and would require significant resource allocations, with the possible exception of terrorism.

In conclusion, Kanuck cautioned against assessing cyberspace from a geographic perspective, pointing out that 21st century geostrategists may find themselves unwilling or unable to pursue the conflicts they desire, either against each other or against their own citizens. The geostrategic implications of cyberspace are real and they are largely unpredictable given the rate of technological advance and its exponential growth; hence the need to question what is being done to maintain collective safety and welfare in cyberspace.

PANEL I

STATE OF THE ART, STATE OF THE WORLD

International Cyber Law and Policy: New Frameworks

Tim Clancy, in addressing international cyber law and the existing policy in place, stated that threats to cybersecurity were becoming increasingly pervasive. He argued that the way to counter them was by reducing the gap between rapidly escalating technological advances and the lagging response from political and social institutions. He emphasised the importance of working towards enhancing our limited ability to assess the actual value of security in cyberspace.

Clancy underscored the need for a multidisciplinary approach for any research agenda related to cybersecurity. He explained that since the cybersecurity agenda could be viewed from many different standpoints – including technical, scientific and geopolitical – often, the discussion around this issue would simply turn out to be a variance of a singular perspective. For instance, at a conference on technology, one would hear a lot about new technological innovations to boost protection in cyberspace, but yet very little on how such innovations could in fact be used or abused in their applications. Similarly, at conferences that deal with the legal or policy aspect of cybersecurity, one would hear a lot about the kinds of technologies which would be permissible by law to increase protection, yet reflect scant research into what could actually be technologically possible or even feasible for execution.

In the legal and policy aspect of cybersecurity, Clancy remarked that "the more things changed, the more things stayed the same". He said that concerns over protecting critical infrastructure systems – essentially cybersecurity in nature because of the networks involved – had been recognised well over twenty years ago; preventing systemic failures back then was very much the same concern as today. However, the same impediments remained when it came to collaborations between the public and private actors across different sectors of society. Although these entities were heavily dependent on cyber networks as internet was crucial to maintaining their daily activities, they were still not sufficiently protected from cyber threats. Nevertheless there was a lack of urgency to cooperate as they were not willing to share information with each other. On the one hand, private organisations like those in telecommunications industry rarely had access to information on threats or vulnerabilities which governments might be exposed to, and *vice versa*.

Additionally, private organisations' dominance and control over the technological means which enhance cybersecurity essentially meant that they (along with their technologies) were also largely beyond the control of governments, further compounding their cooperation issues. Such a reality would only contribute to the tension between ensuring security and delivering efficiency. Clancy believed it was crucial to effectively manage and balance security and efficiency because it was critical for systems like those of telecommunications or grids to not fail or cease to function.

The Low Carbon Energy Cybersecurity Dilemma

Duncan Botting delivered his presentation on the cybersecurity issues from the aspect of energy security. With a particular focus on the west, he examined the dynamics between the lack of change in the physical infrastructure of energy delivery over the past century and the constantly evolving commercial models which have overlaid the existing power systems.

Botting explained that increasing concerns over climate change and security of supply in the past five years or so had changed the commercial model of energy delivery; it had been transformed from one about cost-saving to one driven by a political will to limit the negative impact on the climate and environment. He said the fragmented characteristic of the marketplace in the west – unlike the more vertically integrated state-directed economic structures elsewhere – often had an impact on the delivery of critical services which relied on cyber networks. He cautioned that many of the critical services which depend heavily on energy for electricity are barely being sustained by a flimsy commercial infrastructure. This meant that they were exposed to the danger of being disrupted in the event that the commercial infrastructure collapses. Botting went on to forecast that close to eighty percent of all energy in the future would be delivered by grids which meant the existing physical infrastructure would have to radically change in order to adequately address the changes in generational techniques, e.g. from coal energy to electricity.

Botting argued that cultivating a new mindset was necessary to create cybersecurity resilience and to come up with the policies for developing a framework which could allow markets to deliver the necessary critical services. Information communication technologies (ICT) were needed to overlay the existing infrastructure to activate "smart technologies" which are capable of self-correction. Furthermore, reliability could be enhanced by constructing a distributed architecture because of the fact that systems were distributed by nature. Microgrids, for example, could be used to forge network resilience; the risk could be mitigated by being connected to millions of networks instead of relying on a single network.

Cybersecurity policies needed to take into account new complexities within the environment. Therefore, Botting argued, there was a necessity for both coherence and incoherence to be built into a system to enhance versatility. He posited that this activity of "security by obscurity" could have an important role in the future when technology would constantly be running ahead of policy.

Cybersecurity and International Security

Arvind Gupta spoke on cybersecurity *vis-à-vis* international security. He highlighted three kinds of threats in cyberspace, i.e. cyber crime, cyber terrorism and cyber warfare, each with their own specific sets of policy implications. These kinds of activities in reality remained difficult to categorise, other than in academic journals. As an example, he pointed out that in different contexts, a denial of service (DoS) attack could essentially fall under any one of the three threat categories.

Gupta argued that cybersecurity was emerging as one of the top international security concerns because:

i) the world was becoming increasingly interconnected; ii) cyberspace was constantly evolving; iii) cyberspace had no boundaries; and iv) cyberspace was increasingly becoming an arena for asymmetric warfare. He added that cyberspace has emerged as the fifth dimension of warfare after land, water, air and space.

Gupta urged more international forms of cooperation in cybersecurity. Some of the forms of cooperation already in place included information sharing among states, joint risk management, collaborations among law enforcement agencies, sharing of best practices, cooperation on critical infrastructure protection and 24/7 communications. He also called for further development of international treaties to govern norms in cyberspace as well as voluntary restraint. Most importantly, Gupta argued that since cyberspace was dominated by giant corporations such as Google and Microsoft, governments needed to find ways to effectively collaborate with such profit-driven private organisations by developing new models of public-private cooperation in cyberspace.

Cyberspace Today and Tomorrow – A Singapore's Perspective

Leong Keng Thai spoke on cyberspace and security from the perspective of the Infocomm Development Authority (IDA) of Singapore. As the agency's foremost objective was to help Singapore become globally competitive through the use of ICT, Leong recognised the importance of managing the expanding need for cybersecurity in Singapore.

Leong began by giving an overview of how the internet was developing on a global level. In contrast to the initial stage where the net traffic flow was concentrated in North America, this has gradually been increasingly shifting towards Asia and Europe. He projected that by 2015 there would be 5.8 billion connections in Asia versus 2.3 billion in Western Europe and 2.2 billion in America. Leong said that cyberspace was transforming in a way that social networks, location services, and mobility were all converged together. Furthermore, mobile services appeared to have taken over fixed networks the world over. Unstructured data transaction over the internet stood at about eighty percent which also has implications for cybersecurity.

Leong then looked at Singapore's strategy to increase its global competitiveness through the use of the internet. Over eighty percent of Singaporean households had access to broadband connection, one of the highest in the world. Further, with a mobile internet penetration of 147 percent, Singaporeans were not only using their mobile phones to communicate but to get information on-the-go as well.

Leong explained that the philosophy of the infocomm industry was to promote an open market and competition wherever possible. Accordingly the IDA had worked towards attracting strategic and leading multinational corporations to locate their headquarters and/or offices in Singapore. The IDA also worked with various other agencies to spur innovation through infocomm usage as well as provide support and/or grants for ICT developments and applications. In addition, the IDA linked up to various vertical structures such as health and education. One key area was the establishment of *e-government*. Additionally, they also aimed to develop the *M-government* to address cyber access through mobile networks. IDA also directly engaged with the general public by educating people to become technologically savvy and more aware of cybersecurity issues when using the internet.

Finally, Leong looked at Singapore's strategic approach to developing cybersecurity. Some of the key areas included hardening the infrastructure, identifying key

competencies of those in the cyber sector, developing a vibrant ecosystem and developing international collaborations. Noting that end users were always considered the weakest point of security in cyberspace he said that led the IDA to set up infocomm security awareness programmes among general users, including a Cybersecurity Awareness campaign. IDA also established a code of practice for internet service providers (ISP) operating in Singapore to ensure that they had adequate levels of preparedness in dealing with cybersecurity. IDA also set out measures the ISPs would have to put in place over time to increase their resilience. The IDA also had a Cyber Watch Sector that monitored traffic flowing in and out of government systems as well as their own Computer Emergency Response Team to deal with issues on both international and domestic levels.

Concluding, Leong said that the threats existing in cyberspace are here to stay with us and therefore, we have to face them and come up with a suitable solution. In line with this, he stated that it is crucial to be fully prepared to deal with the dangers and pitfalls of ICT.

DISCUSSION

A participant asked if it was possible to strike a balance between delivering convenience while ensuring security in cyberspace. A speaker agreed that the need to ensure cybersecurity should not be compromised with the usefulness of the internet. He explained it was still important to try to stay ahead of emerging technology even if current efforts to constrain cyberspace were akin to putting a net around things that were essentially uncontrollable. He underscored that as the levels of interconnectivity that existed in cyberspace could not be constrained or interfered with, they necessitated efforts that only sought to contain the abnormal uses of cyberspace, not the normal ones.

Another participant argued that balancing efficiency *vis-à-vis* security needed to be addressed at the local level as the general users had the freedom to make their own decisions. Although there might appear to be great demands for efficiency over security, general users could just as easily demand the improvement of security because the internet essentially remained a realm of private properties. That could give rise to innovative ways to securing the internet without any further government regulation or interference.

PANEL II

ILLICIT ACTIVITIES AND TERRORISM IN CYBERSPACE

Cybersecurity Preparedness in Japan

Motohiro Tsuchiya presented on Japan's cybersecurity preparedness. In 2010, following the arrest of the captain of a Chinese fishing boat off the Senkaku Islands by the Japanese Coast Guards, there were a series of cyber attacks against Japanese websites. However, these attacks caused minimal damage to the websites as the Japanese government was pre-informed about the possibility of these attacks and were able to prepare adequately to deal with them. They had been alerted by the 2009 cyber attacks against websites in South Korea and the US when over 20 government and commercial websites in the US had been targeted by hackers, followed by attacks against South Korean websites.

Cybersecurity has now become an important component of national security in many countries; the US has declared cyberspace as the fifth battlefield. However, there are obstacles faced by governments in ensuring adequate protection against cyber attacks. In an era where technological advances are constantly changing and influencing national security issues, the ability to engage the necessary expertise is of vital importance in a country's national cybersecurity framework. This may prove difficult, given the lucrative return of working for governments and organisations bent on launching attacks.

In Japan, the National Information Security Center (NISC) plays a key role in the nation's cybersecurity framework. However, the NISC does not have intelligence or policing capabilities; its main function is to produce policy and regulations on cybersecurity issues. The Cabinet Intelligence and Research Office (CIRO) is in charge of intelligence but owing to the present organisational structure, both agencies are unable to exchange vital information. Tsuchiya said that this lack of information presented a serious obstacle in the deterrence of cyber attacks. He opined that in order to strengthen the Japanese government's ability to deal with such attacks, widening the scope of intelligence capabilities was important. He concluded that the role of intelligence agencies was vital as part of a country's cybersecurity structure.

Fighting Cyber Crime and Cyberterrorism - A Data-Leakage-Prevention Approach

Anthony Lim's presentation centred on the critical issue of data protection as an important aspect in the prevention of cyber attacks. Data was a critical asset for any organisation or individual and in light of this, there were three main areas of concern in protecting data and mitigating cyber threats: i) software application security; ii) data leakage prevention; and iii) governance.

Lim said that in the area of software application security, an increasingly connected environment exposed the vulnerabilities such as the use of outdated software and poor attitudes in managing security concerns. Despite the presence of firewalls and identity management protocols, cyber terrorists were exploiting weaknesses present in many of the software applications. Current software could be compromised to reveal further information which could be used to allow a person to hack into the entire system. Lim said that this problem often arose because many policies and protocols that have been designed to protect data were not necessarily put into practice and implemented. This created an environment which allows hackers to locate and take advantage of current system weaknesses.

Lim stated that one of the main means of protecting companies against the threat of data security leakage was to ensure that the confidentiality of data entrusted to third party vendors is adequately covered under contractual agreements. Such agreements must have the requisite clauses for the security, continuity, privacy and protection of data. It was also important to ensure that there are existing company policies that cover the loss of items such as laptops, thumb drives and phones which could be used to store valuable data.

Accordingly, there were two components in the provision of cybersecurity, i.e. the technical and the human component. It was noted that most hackers choose to target soft or associated targets. The example of the Wikileaks incident in US highlighted the fact that the loss of data did not involve a technological issue; the information was stolen by an insider using security codes which he had access to. In conclusion, Lim opined that vigilance, diligence, enforcement, education and ownership were crucial in the framework of strengthening cybersecurity.

Illicit Activities and Terrorism in Cyberspace

Zahri Yunos discussed the topic of illicit activities and terrorism in cyberspace and the cybersecurity landscape in Malaysia. Cyber terrorism was seen as the convergence of terrorist motivations and the usage of cyberspace and was generally understood to involve attacks against a particular country's computer and network infrastructures with the aim of intimidating its government and people. Studies conducted by various researchers have found an increase in the number of terrorist and extremist groups using the internet for their activities and to promote their agenda. Among the reasons for such groups choosing this *modus operandi* was its borderless and loosely regulated environment as well as the usefulness and convenience of anonymity in cyberspace.

Yunos said that the propensity for terrorist groups to make use of the internet could lead to the worrying trend of such groups conducting cyber attacks against a country's critical infrastructures. The Malaysian government was acutely aware that any disruptions to the country's critical national infrastructure would have an adverse effect on national security and public safety. Hence, the country's legal framework had provisions stipulating that an attack on critical infrastructures may constitute an act of terrorism.

In terms of Malaysia's cybersecurity governance, a national structure has been put in place to ensure that all the relevant stakeholders are able to operate and coordinate among themselves under one umbrella organisation. One of the main activities undertaken to prepare against and prevent cyber attacks was cyber drills; this was the fourth year that such drills have been conducted on a national level in Malaysia. Despite these steps taken to ensure cybersecurity preparedness, Yunos said that the Malaysian government saw the urgent need for the promotion of cross-border collaboration with other governments for the prevention of cyber attacks. This included the need to address cross-border legislative and jurisdiction issues in combating cyber terrorism.

DISCUSSION

A participant questioned whether there is any difference between cyber crime and cyber terrorism. A speaker replied that cyber crimes involve objectives of gaining dollars and cents whereas cyber terrorists were not motivated by financial incentives. Instead, they were interested in creating chaos, violence and fear. In response to this view, a participant pointed out that while this distinction is clear on paper, a cyber terrorist can also be classified as a cyber criminal. As an example to illustrate this, he mentioned that terrorists often used the internet to raise funds through cyber criminal activities.

A further question was raised whether creation of fear was an absolute factor in constituting cyber terrorism as simply disrupting a particular technological operation could also create fear. A speaker responded that people who would disrupt the technology seldom have commercial objectives in mind; rather, they are likely to be motivated by their own political agenda.

PANEL III

CYBER CONFLICT, CYBER WAR AND CYBER DETERRENCE

War and Peace (Cyber Edition)

Neal Pollard's presentation dealt with the challenges and policy implications of the US government's grand strategy to deal with cyber threats. Of significance was its plan to use the military to deal with severe cyber threats.

Pollard began by identifying three recent initiatives put forth by the US government that underscored its determination to act decisively against cyber threats: i) Department of Defense Strategy for Operating in Cyberspace (July 2011); ii) The Obama Administration's International Strategy for Cyberspace (May 2011); and iii) Creation of US Cyber Command (USCYBERCOM) in 2010[1] .

He then discussed how the military could be deployed in cyber defence. The military would assume a lead role in cyber defence either if it was ordered to by the President or if a cyber attack which involved another state caused severe economic, infrastructural, societal damage or attempted to corrupt the nation's defence systems. In a supporting role, the military would be called upon to use its unique resources such as: i) financial and human resources; ii) technical expertise and operational experience in a security/crisis context; iii) insights into foreign threats, networks, complex planning, training; and iv) access to advance technology to support civilian agencies in a severe cyber attack.

Pollard argued that the military would be used mainly in a supporting role, and therefore it was necessary to identify and attempt to overcome the complex problems which would most likely occur as a result. These problems involved the issue of legal frameworks, policy development, implementation, and so on.

In light of these challenges, Pollard proposed that the US government develop a multiple-agency and multidisciplinary operational framework, which would bridge the gap between military capabilities and those of civilian authorities as well as private sector organisations in cyberspace.

Although attribution was a major determinant of whether countries would respond to a cyber attack in the context of international law, Pollard believed that it was not central to the decision-making process. This was because a country's response would most likely be premised on a geopolitical context and political judgement.

Finally, Pollard commented that as any US' response to a cyber attack would invariably set a precedent in the international arena, the US government should base its response on strategic considerations rather than reactive ones.

[1] USCYBERCOM is a sub-unified command subordinate to US Strategic Command. It plans, coordinates, integrates, synchronises, and conducts activities to: i) direct the operations and defence of specified Department of Defense information networks; ii) prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains; and iii) ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

Legal Paradigms for Cyber Activities

Eric Jensen's presentation focussed on the legal challenges associated with nation versus cyber attacks. He began by assessing the effectiveness of laws at the national, transnational and international levels which deal with malicious cyber activities. Jensen pointed out that malicious cyber activities are normally classified as cyber crime under the law in most countries. As such, legislation to deal with such crimes was well-developed and comprehensive. At the transnational and international levels, however, he argued that legislation was under-developed and severely wanting. As a result, there were no effective legal restraints which would prevent a nation from committing a cyber crime on another nation. Jensen identified three scenarios in which this held true: i) cyber theft; ii) cyber exploitation; and iii) cyber espionage. In these cases, the targeted nation would not have any legal recourse against the attacking nation under international law.

When developing a response to cyber attacks, Jensen pointed out that nations could invoke the law of war as a legal premise for their actions. The law of war governs how states justify their engagement in war *jus ad bellum* as well as how they conduct themselves in war *jus in bello*. Here, the concept of proportionality was important as it essentially regulates the amount of force nations can legally employ if attacked by another state in an actual situation or in cyberspace.

However, even if nations were to invoke the law of war, Jensen argued that it was not a guaranteed solution as there were many grey areas in a legal context which would be problematic. A case in point was the definitional ambiguity of the terms "use of force" and "armed attack" in the context of interstate hostilities. Such ambiguity would ultimately render its application to cyber attacks between states open to broad interpretation.

As existing legal frameworks were inadequate, Jensen opined that a state's response to a cyber attack can be premised on: i) Heat Blast and Fragmentation (HBF) Theory: where the cyber attack has cause an HBF outcome; ii) the Effects Test Theory: where the cyber attack has caused outcomes that equate to a HBF; iii) the US Department of Defense Theory: where the cyber attack has caused a catastrophic event; and iv) Anticipatory and Pre-Emptive Theory: where pre-emptive action is taken as a precaution. He believed that the Effects Test Theory was the most preferred option of the US and its allies.

He concluded by emphasising that while it was desirable to deal with malicious cyber activities through legislation, existing legal frameworks made it impractical for doing so in reality.

Cyber Conflict and the Challenges of Effective Deterrence

Rory Stratton's presentation was an analysis of whether deterrence was possible in cyberspace. He began by observing that many authors and commentators had argued that a major challenge in addressing the threat of cyber attacks was that effective deterrence was difficult, if not impossible, to achieve. This stemmed from the view that even if a state publicly revealed the type of malicious cyber activities which would be within its tolerance threshold and how it would respond to such activities, adversaries would be emboldened rather than deterred from carrying out a cyber attack. Besides, he pointed out, most cyber attacks to date have not resulted in apocalyptic disasters, but rather have simply caused major inconveniences.

Stratton believed that there was a need to reconsider such arguments, especially when one places cyber crime in a geo-political context. He argued that because states possessed numerous and varied forms of reprisals such as economic sanctions, embargoes and kinetic responses, it was unlikely that cyber adversaries would risk provoking retaliation by launching a full-scale cyber attack. Rather, they would commit small-scale nuisance attacks that cause minor disruptions. Stratton opined that the very characteristics of interdependence and unpredictability which place everyone at substantial risk also encourage adversary restraint.

Stratton said cyber attack attribution was difficult, time-consuming, and not always with satisfactory outcome. While cyber forensics had improved, it was still unable to accurately reveal or pinpoint the originator of a cyber attack. Moreover, cyber attackers were also developing new and innovative ways to remain anonymous. An emerging trend which made attack attribution even more challenging was the rise of cyber attack proxies, who had no official affiliation with the state but could be used to carry out cyber attacks on another state, e.g. patriotic hackers.

In conclusion, Stratton suggested that cyber defence should be focussed more on routine cyber crimes such as cyber exploitation, intrusion, and data theft, which are widespread and play a serious role in undermining economies and security, and enabling/facilitating potentially more damaging cyber attacks.

DISCUSSION

A participant asked the speakers whether they could comment on the US government's grand strategy to deal with cyber threats. In particular, this participant wanted to know if other countries should perceive it as an aggressive or benign move on the part of the US. One speaker said that he would not consider the strategy as benign. He stressed that it was premised on defensive rather than offensive considerations with the objective of preventing conflicts within and beyond cyberspace. It is an articulation of how the US and especially the military plans to operate in cyberspace. As for how this strategy should be viewed by allies and adversaries, he opined that it was a declaratory point that the US would consider all options when dealing with cyber attacks. Another speaker added his view that the US' strategy was neither benign nor aggressive but simply reflective of a state's desire to maintain its freedom of action.

A participant raised another question on how the speakers would assess the existing international legislation for cybersecurity and whether it needed to be strengthened to deal effectively with cyber attacks. One speaker expressed his opinion that existing international laws should be strengthened to deal with cyber threats. Another speaker responded that international law pertaining to cyber crimes was untested, and as such, the implications were yet unknown.

Another question posed to the speakers was whether the US government had ensured that systems in the private sector were adequately secured, such that it would deter potential cyber attacks. A speaker responded by saying that the US government was not in the practice of mandating how civilian authorities or agencies secured their systems, although some agencies had embarked on a programme to encourage private sector compliance.

Lastly, a participant asked the speakers to identify the risks of using martial/kinetic metaphors when discussing cyber threats. A speaker responded that the policy issues were mainly at risk from the use of such metaphors, and the aims for their use were mainly political. He opined that such metaphors had very little impact on the laws governing cyber threats. Another speaker believed that such metaphors were detrimental as they provoked emotional responses rather than rational assessments of cyber threats.

PANEL IV

STRATEGIC COMMUNICATIONS AND PUBLIC DIPLOMACY IN CYBERSPACE

The Impact of New Media on Strategic Communications in Cyberspace

Matt Armstrong addressed the manner in which the current dynamics between the cyberspace environment and people affect the states' struggle to win the minds and wills of the people. Armstrong noted that the use of the mass media by the state to communicate messages to the people is not a new phenomenon. However, the failure to do so effectively in the current context is likely to result in far greater consequences than in the past, given the ubiquity of information technology in the present.

Armstrong depicted the present information environment – or Now Media – as follows: i) it is democratic; ii) it bypasses traditional hierarchies while creating new ones; and iii) it alters traditional concepts of trust and accountability. Given this situation, organisations and governments are faced with challenges as they navigate in this dynamic environment where perceptions could trump reality. Nevertheless, states ignore this phenomenon at their own peril as their failure to engage in this domain may result in the loss of their initiative to shape the key narratives critical to winning the minds and wills of the people.

Armstrong went on to outline the three points to consider when preparing to engage the modern human and information environment. First, additional communication pathways paved by the information environment bypass and challenge the authority of governments. Moreover, increased connectivity not only reduce the demand for people to assimilate into local environments outside cyberspace but also facilitates "turnstile allegiance" as individuals are no longer dependent on a shared history, culture, ethnicity or language for a sense of belonging. Instead, they may form new transnational communities based on common interests. Hence there is a need to rethink the notion of national allegiance in the present context. Second, states need to clearly identify the audience they seek to engage and how to engage them. For instance, one needs to consider the optimal balance between the use of traditional and new media when reaching out to the different segments of society. Governments also need to be mindful of their adversaries' strategies to undermine the state *via* new media. Third, there is a need to develop various measures to assess the effectiveness in attaining one's goal when engaging the masses in cyberspace.

In conclusion, in order to effectively manage the public sentiment in the modern human and information environment, states need to educate, empower, equip and encourage those within their ranks to navigate it.

Social Media and its Impact to a Government's Strategic Communication

Nicolas Ojeda examined the impact of social media on strategic communication by focussing on the example in the Philippines.

Ojeda began with the definition of strategic communications as "the delivery of messages by the government to the public to achieve positive changes in perception, attitude and behaviour". This entails implementing programmes and activities deliberately aimed at communicating and engaging with the target audiences. In this endeavour, careful attention has to be paid to the synchronisation of words and deeds such that the message is transmitted effectively as intended.

Ojeda went on to examine the manner in which social media posed challenges to government efforts in the area of strategic communications and public diplomacy. First, the speed at which social media allows for information to be disseminated requires the state to respond to the situation in a timely manner. Second, social media platforms facilitate the shaping of perceptions and views on a range of issues, especially among youths, which may be used to mobilise the masses to challenge the status quo. Third, the uncontrolled nature of social media and the lack of accountability for its contents as users may remain anonymous and post unreliable information means that the state will have to be constantly alert in order to rectify misinformation.

Nevertheless, if wielded effectively, social media may also serve as an effective tool of strategic communication between governments and citizens. To illustrate this point, Ojeda listed a few examples of the Philippines government's usage of social media, such as Facebook and Twitter, as follows: i) diplomats used them to share glimpses of their personal lives with the public; ii) politicians employed them to advance their agendas; iii) government agencies used them to disseminate information to the public; and iv) military units used them to facilitate civil-military operations.

In conclusion, the capacity of new media to spread information and mobilise the masses has rendered it impossible for governments to insulate their citizens from local, regional and global trends. In line with this, Ojeda opined that governments must also learn to embrace the new media and utilise its strength for strategic communications in order to engage their citizens more effectively.

Statecraft in Cyberspace: Bring in the State Back

Kusnanto Anggoro discussed the challenges states faced in regulating cyberspace based on the Indonesian case study. He argued that modern technology itself is merely a strategic tool to be employed by various state and non-state actors to achieve their desired goals. The real challenge of modern technology emerges from the uneven distribution of available resources and capabilities both within and among states.

Anggoro pointed out that anarchy in cyberspace creates more uncertainty than anarchy in traditional inter-state relations. This is because anarchy in traditional inter-state relations often hinges on the balance of power in which there are clear indicators whether or not an opponent is a threat, such as its military capacity. However, cyberspace can be both an enabling and disruptive agent depending on how it is harnessed. Hence it is difficult to decide whether a certain identified trend in cyberspace will enhance or undermine a state's capacity.

In Indonesia, there is a general consensus that the capacity of the state to deal with the challenges of cybersecurity needs to be enhanced although the means to do so is disputed. Anggoro identified several key areas for the Indonesian authorities to develop, namely enhancing the professional competence of state agencies and developing sustainable institutions and legal frameworks for enforcement. There also needs to be clearer national objectives pertaining to cybersecurity, better coordination among the different state agencies, and strengthening of bonds of trust between the state and society. In conclusion, Anggoro summarised that under the anarchic condition of cyberspace, cooperation was crucial in order to enhance cybersecurity.

The Role of "Purposeful Attribution" and "Active Deterrence" in Cyberspace

Daniel Arista discussed the role of "purposeful attribution" and "active deterrence" in managing the risk inherent with operating an IT infrastructure. This, he argued, required an understanding of system vulnerability and how they could be exploited.

Purposeful attribution is necessary for pursuing applications of justice and national interests legitimately while active deterrence facilitates the optimisation of the welfare cyberspace provides. Deterrence can best be achieved by not being overly vulnerable and also by letting one's adversaries know we can attribute their acts to them. However, developing the capability to retaliate is likely to create a mix of cyber and kinetic effects. Hence building cyber-offensive capability is not a good strategy for deterrence as it merely adds more munitions and technical options of how one might retaliate.

Arista observed that the knowledge and capacity to be better at attribution and lowering vulnerability was currently available yet not acted upon. He attributed this to a lack of incentive to do so. For instance, he noted that the vast majority of the networks were maintained by the private sectors and that functionality was prioritised over security. In order to overcome this situation, there is a need to create better incentives for cybersecurity, which entails instituting accountability. This would involve having the software industry and the network providers to take a stake in internalising some of the costs of operating a vulnerable network.

Implementing accountability should entail the following considerations: i) What is a reasonable risk one can take when operating in cyberspace?; ii) What is a vendor's liability when they buy and sell software, hardware and accessibility to networks?; and iii) How can norms of responsibility be imbued in individuals such that they do not put others on the same network as them at risk?

In conclusion, the demand for cybersecurity will not occur naturally but must be induced with liability, which can be leveraged to promote accountability and stimulate the incentive for the desired risk management in cyberspace.

DISCUSSION

A participant noted that the recent spate of challenges to the stability of governments, such as the Arab Spring, has often been attributed to changes in societal norms and the increasing ubiquity of social networking technology. He asked whether there were other possible causes for this phenomenon and how the different factors involved would change the rules of engagement between government and citizens. One speaker was of the opinion that cultural values differed along both generational and technological divides. He noted that the younger and more technologically savvy generations were more comfortable expressing democratic and liberal views. However, this has created a gap between the older and younger generations as the older generation, including many in government, have difficulty connecting with the youths. Other speakers added that while social networks provide a platform for people to organise themselves, it is merely a facilitator and not a key driver.

Another participant asked for an assessment of the geostrategic impact of social media, namely whether the increased connectivity over the last few years has resulted in more or less stability, and also the implications on civil rights, liberties, and privacy. A speaker believed that while social media has the potential to have both a positive and negative effect on social stability, the net effect would be positive. Most of the gains would pertain to civil rights and liberties as governments will be forced to be more transparent and accountable. However, the net impact on privacy was likely to be negative. Even though the proliferation of such networks may result in an initial period of instability, for instance the Middle East at present, he believed the impact would be a net positive in the long run. He also stressed that governments have to participate in shaping public opinion in cyberspace or risk losing this initiative to their adversaries. Another speaker concurred and noted that many politicians and diplomats were beginning to engage the public through social media platforms such as Facebook. On the negative impact of social media on privacy, a speaker added that the problem can be mitigated through a more discerning use of the existing technology and platforms. For instance, one could create multiple Facebook accounts for different purposes and audiences to reduce the incidences of sensitive or private information being inadvertently disclosed to unintended audiences.

PANEL V

THE WAY FORWARD

Cybersecurity Futures: Charting a Path for Policy Development

Ruth David began the discussion by mentioning the inability of the current legal systems to adequately address the complex issue of security in cyberspace. For this reason, she proposed a multidisciplinary approach which blends the current legal frameworks with the existing laws governing cyberspace in order to address the unique aspects of cyberspace and its emerging trends.

David stated that the concept of "cyberspace" emerged as a buzz term in 1984 which, at the time merely referred to the most basic computer networks. Overtime, this evolved into a more complicated critical infrastructure beyond a mere IT infrastructure as can be observed today. The significance of cyberspace also comes from its interdependent transactional capability. David opined that the issue of cybersecurity is not only the question of what it is now, but how it will transform in the near future. David said that cyberspace is now emerging as a complex domain which affects anyone, anywhere, at any time.

To summarise, the concept of cybersecurity went through a gradual transition in the following order: computer security, network security, internet security, and newly emerging security issues derived from cyberspace. David said that the concept will keep evolving and it is imperative to protect certain assets which are crucial for cybersecurity, i.e. IT infrastructure (hardware and software), data, functionality, and transactional capability.

Currently, there are international and regional standards and policies to monitor cyber threats, such as those of the Council of Europe, United Nation, Global Network Initiative and Society for the Policing of Cyberspace. These standards and policies were largely based on the existing guidelines and principles to enhance cybersecurity. David opined that they must also be able to adopt and adapt the emerging norms and policies to address the complexity and progressive nature of cyberspace.

David concluded her presentation by stating that it was crucial to devise a more responsive and effective set of policies in order to catch up with the rapidly evolving trend of cybersecurity. To illustrate this, she shared a framework developed by one think-tank in Washington which suggested the following six crucial steps to enhance cybersecurity: i) identify the different levels of stakeholders; ii) build international collaboration among nations; iii) clarify international norms; iv) establish accountability; v) expand the community; and vi) foster international standards.

Cybersecurity: The Way Forward from a US Perspective

Sean Kanuck conceptualised four key elements in cyberspace security; threats, values, norms and risks. First, he said that different kinds of threats in cyberspace needed to be constantly monitored and dealt with as far as cybersecurity was concerned. Kanuck opined that in terms of cybersecurity, terrorism is one of the most challenging threats which threaten the cyberspace. In terms of values, the speaker said that it concerns the question of what we are trying to protect, from whom, and why. Thirdly, Kanuck proposed taking the existing norms together with the emerging ones which could

adequately address the evolving trend of cybersecurity. Lastly, Kanuck reminded that the risks in cyberspace are real and they need to be thoughtfully addressed to ensure the security of cyberspace.

Kanuck concluded that there are three important things in order to move forward to ensure cybersecurity: i) people matter in terms of the values and the knowledge possessed; ii) standards are important in order to understand the rules of the game; and iii) precedents matter as they enable us to learn from others' experiences in tackling challenges in cyberspace.

Cybersecurity: The Way Forward from a Singaporean Perspective

Peter Ho began his discussion by consciously affirming that the cybersecurity is a real problem, not just a virtual one. He opined that the most severe cyber attack was Stuxnet (2010) because it has resulted in physical damages which extended beyond the destruction of the virtual infrastructure. Cyber attacks targeted at vulnerabilities which exist in government systems were presumed to be the emerging trend which required a set of skilled capabilities to overcome such challenge.

Ho opined that the evolution of cyberspace is associated with the possibility of increased connectivity and interdependency which would render the critical infrastructure even more vulnerable to cyber attacks. On the benefits gained from this trend in cyberspace, he noted that as the cyberspace expanded in capability and interconnectivity, the Z generation has benefitted in terms of convenience by "consumerising IT". In addition, the modern world has benefitted from the internet through its innovative technologies which has also contributed to forming a globalised community.

On the other side, Ho said that the evolution of cyberspace has also brought its own side effects. A lack of stringent regulations in cyberspace allowed adversaries with malicious intent to plan and spread their hate-ideologies. Moreover, this was facilitated by anonymity which enabled them to conceal their identities. Another major challenge of the internet lay in the asymmetrical position between the defender and attacker in cyberspace. In other words, while the defender often did not possess adequate capability to strongly respond to a cyber attack, an attacker usually did not require much resource to carry it out.

Some countries, such as India and US, applied customised national regulations in order to secure the cyberspace. This basically derived from the notion of considering internet as a national asset. However, it is impossible to avoid every undesired consequence because cyber threats could

originate from anywhere around the world due to its borderless nature. Therefore, it would be better to develop a global regulation rather than national regulations in order to better address the issue of cybersecurity. With regard to forming a global regulation for cybersecurity, there were two main issues which must be considered. First, it is extremely difficult to balance regulations with freedom to access information on the internet as it is impossible to entirely block access to all contents which exist online. Second, the industry and the community should devise the common rules and regulations which would cultivate the culture of self-regulation and prevent cyber threats from reaching its targets.

As an example of how Singapore endeavours to enhance its cybersecurity, Ho shared the main roles of Singapore's National Infocomm Security Committee as follows: i) strike a balance between national security and economy; ii) undertake the risk management measurements to minimise destructive possibilities; iii) develop masterplans to build capacity by recruiting experts in cyber infocomm security through scholarships and supporting the R&D team in order to maintain the interdependencies of critical infrastructures; and iv) establish the cybersecurity organisation for policy development and as a centre for command and control.

As the landscape of cyberspace is constantly changing and threats are becoming more lethal for cybersecurity, it was recommended that the international community rigorously involve grassroot organisations to take part in its endeavour to enhance security in cyberspace.

Cybersecurity: The Way Forward from an Indian Perspective

Arvind Gupta opined that cybersecurity evolved into an international issue as a result of the transition in international order after the Cold War. He also said that the world has witnessed more overlapping of traditional and non-traditional security in which different threats arising from different sources cannot be considered as separate matters. Gupta stated that while the power of cyberspace has greatly contributed to political and economic prosperity, it has also created more opportunities for state and non-state actors to execute their malicious plans and actions. He added that there is a growing collaboration between state and non-state actors in this regard.

In conclusion, Gupta opined that cyberspace has become part of the global commons and therefore, international collaboration and public diplomacy were greatly required in order to maintain political and economic prosperities.

DISCUSSION

A participant asked how the local regulations on cyberspace within a particular country would apply to a multinational entity, e.g. multinational corporations. A speaker responded that a standard practice for multinational corporations in terms of cybersecurity would be to abide by their own in-house regulations. He added that international standards could also be applied depending on the situation but generally, local regulations would apply if a cyber crime was carried out within a particular country by a multinational corporation.

Another participant asked what the speakers thought the main factor of a cyber attack would be. A speaker answered that rather than dissecting the factors of cyber attack one by one, it would be better to understand the overall structure of cyberspace as a whole. He opined that among all elements which constitute this structure, human factor was the most vulnerable to cyber threats.

WORKSHOP AGENDA

Sunday, 17 July 2011

1700 – 1800 **Arrival of Invited Foreign Participants and Speakers**

Venue: Marina Mandarin Hotel

1800 – 2000 **Welcome Reception**

Hosted by ***Cung Vu***, *National Maritime Intelligence Center and Global Futures Forum, Department of State and* ***Bilveer Singh***, *Acting Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Venue: Tambuah Mas Indonesian Restaurant

Monday, 18 July 2011

0800 – 0830 **Registration**

0830 – 0840 **RSIS Corporate Video**

0840 – 0900 Welcome Remarks by *Cung Vu, National Maritime Intelligence Center and Global Futures Forum, Department of State* and *Bilveer Singh, Acting Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Venue: Vanda Ballroom (Level 5)

Attire: Smart Casual (Long-sleeve shirt without tie)

0900 – 0930 **Keynote Speech**

"Cybersecurity Frameworks"
by ***Sean Kanuck***, *National Intelligence Officer for Cyber Issues, National Intelligence Council*

0930 – 1000 Coffee Break

1000 – 1130 **Panel 1: State of the Art, State of the World**

Venue: Vanda Ballroom (Level 5)

Chairperson:
Cung Vu, *National Maritime Intelligence Center and Global Futures Forum, Department of State*

Speakers:
"International Cyber Law and Policy: New Frameworks" by ***Tim Clancy***, *Senior Cybersecurity Policy Analyst, Syracuse Research Corporation (SRC) Inc.*

"The Low Carbon Energy Cybersecurity Dilemma" by ***Duncan Botting***, *Business Innovation and Growth Director, Parsons Brinckerhoff, UK*

"Cybersecurity and International Security" by ***Arvind Gupta***, *Lal Bahadur Shastri Chair, Institute for Defence Studies and Analyses (IDSA), India*

"Cyberspace today and tomorrow – A Singapore's perspective" by ***Leong Keng Thai***, *Deputy Chief Executive Officer & Director-General (Telecoms & Post), Infocomm Development Authority of Singapore*

1130 – 1230

Panel 2: Illicit Activities and Terrorism in Cyberspace

Venue: Vanda Ballroom (Level 5)

Chairperson:
Bilveer Singh, *Acting Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers:
"Cybersecurity Preparedness in Japan: Response to the 2009 Attacks on South Korea and the United States" by ***Motohiro Tsuchiya***, *Professor, Keio University, Japan*

"Fighting Cyber Crime and Cyberterrorism – A Data-Leakage-Prevention Approach" by ***Anthony Lim***, *Director, IBM, Singapore*

"Illicit Activities and Terrorism in Cyberspace" by ***Zahri Yunos***, *Chief Operating Officer, Cybersecurity Malaysia*

1230 – 1330

Lunch
Venue: Leo Ballroom (Level 1)

1330 – 1500

Breakout Sessions
(Syndicate Sessions to cover topics covered in panel 1&2)

Attire: Smart Casual (Long-sleeve shirt without tie)

Group 1 & 2: Vanda Ballroom (Level 5)

Group 3 & 4: Taurus Ballroom (Level 1)

1500 – 1530

Coffee Break

1530 – 1600

Syndicate Group Presentation
Venue: Vanda Ballroom (Level 5)

1600 – 1715

Panel 3: Cyber Conflict, Cyber War and Cyber Deterrence

Venue: Vanda Ballroom (Level 5)

Chairperson:
Motohiro Tsuchiya, *Professor, Keio University, Japan*

Speakers:
"War and Peace (Cyber Edition)" by ***Neal Pollard***, *Principal, PRTM Management Consultants*

"Legal Paradigms for Cyber Activities" by ***Eric Jensen***, *Law Professor, Fordham University*

"Cyber Conflict and the Challenges of Effective Deterrence" by ***Rory Stratton***, *Foreign Affairs Officer, Office of Cyber Affairs, Bureau of Intelligence and Research, US State Department*

1800 – 2000

Workshop Dinner
Venue: Aquamarine @ Level 4

Attire: Smart Casual
(Long-sleeve shirt without tie)

Wednesday, 19 July 2011

0845 – 0900	Review of Day 1
0900 – 1030	**Panel 4: Strategic Communications & Public Diplomacy in Cyberspace** Venue: Vanda Ballroom (Level 5) Attire: Smart Casual (Long-sleeve shirt without tie) Chairperson: ***Zahri Yunos**, Chief Operating Officer, Cybersecurity Malaysia* Speakers: ***Matt Armstrong**, Executive Director, US Advisory Commission on Public Diplomacy* ***"Social media and its impact to a Government's Strategic Communication"*** by ***Nicolas Ojeda** Jr, Brigadier General (Ret), Philippine Institute for Peace, Violence, and Terrorism Research, Philippines* ***"Statecraft in Cyberspace: Bring in the State Back"*** by ***Kusnanto Anggoro**, Lecturer, University of Indonesia* ***Daniel E. Arista**, Principal Cybersecurity Research Scientist, Advanced Technology Initiatives Program, SRC Inc.*
1030 – 1100	Coffee Break
1100 – 1230	Breakout Sessions (Syndicate Sessions to cover topics covered in panel 3&4) Group 1 & 2: Vanda Ballroom (Level 5) Group 3 & 4: Taurus Ballroom (Level 1)
1230 – 1330	Lunch Venue: Leo Ballroom (Level 1)
1330 – 1400	Syndicate Group Presentation Venue: Vanda Ballroom (Level 5)
1400 – 1600	**Panel 5: The Way Forward** Venue: Vanda Ballroom (Level 5) Chairperson: ***James Kadtke**, Industry and State Liaison, National Nanotechnology Coordinating Office* Speakers: ***"Cybersecurity Futures: Charting a Patch for Policy Development"*** by ***Ruth David**, CEO, Anser Inc.* ***"Cybersecurity: The Way Forward from a US Perspective"*** by ***Sean Kanuck**, National Intelligence Officer for Cyber Issues, National Intelligence Council* ***"Cybersecurity: The Way Forward from a Singaporean Perspective"*** by ***Peter Ho**, Senior Advisor, Centre for Strategic Futures, Singapore* ***"Cybersecurity: The Way Forward from an Indian Perspective"*** by ***Arvind Gupta**, Lal Bahadur Shastri Chair, Institute for Defence Studies and Analyses (IDSA), India*
1600 – 1620	Coffee Break
1620 – 1700	Day 2: Wrap-up

ABOUT CENS

The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

WHY CENS?

In August 2004 the Strategic Framework for National Security outlined the key structures, security measures and capability development programmes that would help Singapore deal with transnational terrorism in the near and long term.

However, strategising national security policies requires greater research and understanding of the evolving security landscape. This is why CENS was established to increase the intellectual capital invested in strategising national security. To this end, CENS works closely with not just other RSIS research programmes, but also national security agencies such as the National Security Coordination Secretariat within the Prime Minister's Office.

WHAT RESEARCH DOES CENS DO?

CENS aspires to be an international research leader in the multi-disciplinary study of the concept of resilience in all its aspects, and in the policy-relevant application of such research in order to promote security within and beyond Singapore.

To this end, CENS conducts research in three main domains:

Radicalisation Studies

- *The multi-disciplinary study of the indicators and causes of violent radicalisation, the promotion of community immunity to extremist ideas and best practices in individual rehabilitation. The assumption being that neutralising violent radicalism presupposes individual and community resilience.*

Social Resilience

- *The systematic study of the sources of – and ways of promoting – the capacity of globalised, multicultural societies to hold together in the face of systemic shocks such as diseases and terrorist strikes.*

Homeland Defence

- *A broad domain encompassing risk perception, management and communication; and the study of best practices in societal engagement, dialogue and strategic communication in crises. The underlying theme is psychological resilience, as both a response and antidote to, societal stresses and perceptions of vulnerability.*

HOW DOES CENS HELP INFLUENCE NATIONAL SECURITY POLICY?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organises courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

HOW DOES CENS HELP RAISE PUBLIC AWARENESS OF NATIONAL SECURITY ISSUES?

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence-related publications, as well as write op-ed analyses in leading newspapers. Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as radicalization and counter-terrorism, multiculturalism and social resilience, as well as risk management and mitigation.

HOW DOES CENS KEEP ABREAST OF CUTTING EDGE NATIONAL SECURITY RESEARCH?

The lean organisational structure of CENS permits a constant and regular influx of Visiting Fellows of international calibre through the Distinguished CENS Visitors Programme. This enables CENS to keep abreast of cutting edge global trends in national security research.

For more information on CENS, log on to **http://www.rsis.edu.sg** and follow the links to "Centre of Excellence for National Security".

ABOUT GFF

WHAT IS THE GFF?

The **Global Futures Forum (GFF)** is a multinational community initiated in 2005 that works at the unclassified level to make sense of emerging and future transnational and global security challenges. Its primary goal is to foster the development of enhanced insight and foresight among its membership through the exchange of diverse perspectives and through the utilisation of collaborative analytic tools.

WHO IS THE GFF?

GFF seeks to involve a diverse population of governmental and private sector subject matter experts to stimulate cross-cultural and interdisciplinary thinking and to challenge prevailing assumptions. Membership in the GFF is limited to governmental intelligence organisations and other governmental organisations focussed on foreign, internal, or international security issues. All such organisations regularly seek to monitor, understand, and forecast threats to national and international security as either their main line of work or as an ancillary function to policy formation or operations. GFF participants include analysts from intelligence, diplomatic, defence, and homeland security agencies, along with counterparts from academia, non-government organisations, and industry. More than 1,500 officials and experts from over 50 countries have taken part in GFF activities to date.

Argentina	**EUROPOL****	**Lithuania**	**Slovakia**
Australia*	**Finland***	**Luxemburg**	**South Africa**
Austria*	**France***	**Malaysia**	**South Korea**
Bangladesh	**Germany**	**Mexico**	**Spain**
Belgium*	**Greece**	**New Zealand**	**Sweden***
Brazil	**Hungary***	**Norway**	**Switzerland***
Brunei	**India**	**Panama**	**The Netherlands***
Bulgaria	**Indonesia**	**Philippines**	**Trinidad & Tobago***
Cambodia	**Ireland**	**Poland***	**Turkey**
Canada*	**Israel**	**Portugal***	**United Arab Emirates**
Chile	**Italy***	**Romania***	**United Kingdom***
Czech Republic*	**Japan***	**Singapore***	**United States***
Denmark*	**Jordan**		**Vietnam**
Estonia	**Latvia***		

*** Member Countries**

**** Observer**

HOW DOES THE GFF WORK?

General meetings: Washington, November 2005; Prague, December 2006; Vancouver, April 2008, and Singapore, September 2010.

Community of Interest (COI) workshops - small topic-based meetings held regularly in various member countries.

GFF operates a password-protected website that serves as the repository of reports from GFF workshops. It also includes hundreds of readings and resources on relevant topics, member blogs, discussion forums, and wikis: www.globalfuturesforum.org.

WHAT ARE THE GFF COIS? THE SEVEN (7) COIS FOCUS RESPECTIVELY ON:

- Emerging and Disruptive Technologies	- Proliferation
- Human and Natural resource Security	- Radicalisation and Counter-terrorism
- Illicit Trafficking	- Strategic Foresight and Warning
- Practice and Organisation of Intelligence	

For more information on GFF, please write to admin@globalfuturesforum.org.

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** was officially inaugurated on 1 January 2007. Before that, it was known as the Institute of Defence and Strategic Studies (IDSS), which was established ten years earlier on 30 July 1996. Like its predecessor, RSIS was established as an autonomous entity within the Nanyang Technological University (NTU).

The School exists to develop a community of scholars and policy analysts at the forefront of Asia Pacific security studies and international affairs. Its three core functions are research, graduate teaching and networking activities in the Asia Pacific region. It produces cutting-edge security related research in Asia Pacific Security, Conflict and Non-Traditional Security, International Political Economy, and Country and Area Studies.

The School's activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific and their implications for Singapore.

For more information about RSIS, please visit **http://www.rsis.edu.sg/**

ABOUT NSCS

The **National Security Coordination Secretariat (NSCS)** was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is Deputy Prime Minister and Minister for Home Affairs Mr. Teo Chee Hean.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr Peter Ong, who is concurrently Head of Civil Service, Permanent Secretary (Finance) and Permanent Secretary (Special Duties).

NSCS is made up of two components: the National Security Coordination Centre and the Joint Counter Terrorism Centre. Each centre is headed by a director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipating strategic threats. As a coordinating body, NSCS ensures that government agencies complement each other, and do not duplicate or perform competing tasks. It also organises and manages national security programmes, one example being the Asia-Pacific Programme for Senior National Security Officers, and funds experimental, research or start-up projects that contribute to our national security.

For more information about NSCS, visit **http://www.nscs.gov.sg/**

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

A Graduate School of Nanyang Technological University

S. Rajaratnam School of International Studies, Nanyang Technological University,
Block S4, Level B4, Nanyang Avenue, Singapore 639798
TEL 65-6790-6982 | FAX 65-6793-2991 | EMAIL wwwrsis@ntu.edu.sg | WEBSITE www.rsis.edu.sg

Design by Oxygen Studio Designs